BGD Siber Güvenlik ve Savunma Kitap Serisi 4

Siber Güvenlik ve Savunma

BİYOMETRİK VE KRİPTOGRAFİK UYGULAMALAR

Editörler

Prof. Dr. Şeref Sağıroğlu

Doç. Dr. Sedat Akleylek

nobel

SİBER GÜVENLİK VE SAVUNMA
Biyometrik ve Kriptografik Uygulamalar

Editörler: Prof. Dr. Şeref Sağıroğlu - Doç. Dr. Sedat Akleylek

Yayın No. : 3229
Mühendislik/Teknik No : 332
ISBN : 978-625-439-024-1
E-ISBN : 978-625-439-025-8
Basım Sayısı : 1. Basım, Aralık 2020

Genel Yayın Yönetmeni : Nevzat Argun -nargun@nobelyayin.com-
Yayın Koordinatörü : Gülfem Dursun -gulfem@nobelyayin.com-

Redaksiyon : Buse Gamze Çeliktaş -buse@nobelyayin.com-
Sayfa Tasarım : Tarkan Kara -erdal@nobelyayin.com-
Kapak Tasarım : Grafiker
Baskı Sorumlusu : Yavuz Şahin -yavuz@nobelyayin.com-
Baskı ve Cilt : Sarıyıldız Ofset Amb. Kağ. Paz. San. ve Tic. Ltd Sertifika No.: 23593
İvedik Ağaç İşleri San. Sit. 1354. Cad. 1358. Sok. No.: 31 Ostim / ANKARA

Kütüphane Bilgi Kartı

Sağıroğlu, Şeref., Akleylek, Sedat.
Siber Güvenlik ve Savunma Biyometrik ve Kriptografik Uygulamalar / *Şeref Sağıroğlu - Sedat Akleylek*
1. Basım. XVIII + 508 s. 16x23,5 cm. Kaynakça ve dizin var.
ISBN: 978-625-439-024-1
E-ISBN: 978-625-439-025-8
1. Sis Bilişimi ve Uygulamalarında Veri Güvenliği 2. Saldırı Tespit Sistemleri ve LOG (Günlük) Analizi 3. Açık Kaynak İstihbaratı (Open Source Intelllgence OsInt) 4. Biyolojik Biyometrik Sistemler, Biyometrik Veriler, Hukuk ve Güvenlik 5. Davranışsal Biyometrik Sistemler, Teknolojiler ve Güvenlik 6. Biyometride Yeni Nesil Davranış Modelleme Yaklaşımları, Riskler ve Öngörüler 7. Kafes Tabanlı Kriptografide Kullanılan Zor Problemlerin Kriptanalizi ve Yazılım Kütüphaneleri 8. Ağ Anomali Tespitinde Makine Öğrenmesi Algoritmalarının Kullanılması ve Sınıflandırma İçin Bir Uygulama Örneği 9. Kriptografik Blok Şifrelerin Maksimum Uzaklıkla Ayrılabilen Yayılım Tabakalarının Tasarımı 10. Güvenlik Uygulamalarını Hedefleyen Fiziksel Saldırılar ve Bunlara Karşı Alınabilecek Önlemler 11. Küresel Salgının Ulusal Bilişim Güvenliğine Etkileri 12. DevSecOps 13. Endüstriyel Kontrol Sistemlerinin Siber Güvenliği 14. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sisteminde Karşılaşılan Uygulama Zorlukları 15. Siber Tehdit İstihbaratı ve Saldırı Tespit Sistemlerinde Büyük Veri Teknolojileri

Genel Dağıtım

ATLAS AKADEMİK BASIM YAYIN DAĞITIM TİC. LTD. ŞTİ.
Adres: Bahçekapı mh. 2465 sk. Oto Sanayi Sitesi No:7 Bodrum Kat Şaşmaz-ANKARA - siparis@nobelyayin.com-
Telefon: +90 312 278 50 77 - **Faks:** 0 312 278 21 65
E-Satış: www.nobelkitap.com - esatis@nobelkitap.com / www.atlaskitap.com - info@atlaskitap.com

Dağıtım ve Satış Noktaları: Alfa Basım Dağıtım, Arasta, Arkadaş Kitabevi, D&R Mağazaları, Dost Dağıtım, Ekip Dağıtım, Kida Dağıtım, Kitapsan, Nezih Kitabevleri, Pandora, Prefix, Remzi Kitabevleri

BÖLÜM YAZARLARI

Bölüm 1
Sis Bilişimi ve Uygulamalarında Veri Güvenliği
SEDAT AKLEYLEK - AYKUT KARAKAYA

Bölüm 2
Saldırı Tespit Sistemleri ve LOG (Günlük) Analizi
HİDAYET TAKCI

Bölüm 3
Açık Kaynak İstihbaratı (Open Source Intelligence Osint)
HÜSEYİN AKARSLAN

Bölüm 4
Biyolojik Biyometrik Sistemler, Biyometrik Veriler, Hukuk Ve Güvenlik
PELİN ÖZKAYA - REFİK SAMET

Bölüm 5
Davranışsal Biyometrik Sistemler, Teknolojiler ve Güvenlik
HANDE TUTUMLUER - REFİK SAMET

Bölüm 6
Biyometride Yeni Nesil Davranış Modelleme Yaklaşımları, Riskler ve Öngörüler
BİLGEHAN ARSLAN - ÇAĞLA AKSOY - ŞEREF SAĞIROĞLU

Bölüm 7
Kafes Tabanlı Kriptografide Kullanılan Zor Problemlerin Kriptanalizi ve Yazılım Kütüphaneleri
HAMİ SATILMIŞ - SEDAT AKLEYLEK

Bölüm 8
Ağ Anomali Tespitinde Makine Öğrenmesi Algoritmalarının Kullanılması ve Sınıflandırma İçin Bir Uygulama Örneği
HABİBE GÜLER - ŞEREF SAĞIROĞLU

Bölüm 9
Kriptografik Blok Şifrelerin Maksimum Uzaklıkla Ayrılabilen Yayılım Tabakalarının Tasarımı
MELTEM KURT PEHLİVANOĞLU - ELİF BİLGE KAVUN

BİLGİ GÜVENLİĞİ DERNEĞİ'NDEN

Bilgi Güvenliği Derneği (BGD); 22.07.2007 tarihinde, Bilgi Güvenliği ve Siber Güvenlik alanında toplumun her kesiminde bilgi ve bilinç düzeyini arttırmak, bu konu ile ilgili teknolojik gelişmeleri izlemek, yerli ve milli teknolojilerin geliştirilmesine katkı sağlamak; bireysel, kurumsal ve ulusal düzeydeki riskler konusunda farkındalık oluşturmak ve kamu-sektör-üniversite işbirliklerini geliştirmek amacı ile kurulmuştur.

BGD'nin vizyonu; "bilgi güvenliği alanında ulusal ve uluslararası düzeyde tarafsız, güvenilir ve etkin bir ulusal sivil toplum kuruluşu olmaktır." BGD amacı doğrultusunda; tüm paydaşlarla işbirliği yaparak mevzuatın oluşturulmasında ve geliştirilmesinde aktif rol almakta, gerçekleştirdiği konferans, sempozyum, çalıştay ve eğitimler, yayımladığı rapor ve yazılar ile farkındalığın oluşmasına ve bunun davranışa dönüştürülmesine katkılar sağlamaktadır.

Derneğimiz bu kapsamda; "Ulusal Siber Güvenlik Strateji Belgesi" ve "Ulusal Siber Güvenlik Eylem Planı" hazırlanmasına öncülük etmiş, hazırladığı taslak metinler kabul görmüş ve sonuçta ülkemizin siber güvenlik stratejisi ve eylem planlarının gecikmeden yayımlanasına katkı sağlamıştır. Aynı zamanda; bu alanda nitelikli insan kaynağı yetiştirilmesi, mesleki yeterliliklerin belirlenmesi, kamu-endüstri-üniversite işbirliklerinin geliştirilmesi, kümelenme çalışmalarının başlaması gibi önemli politika ve stratejilerin oluşturulmasında etkin rol üstlenmektedir.

BGD, "Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı", "Ulusal Siber Güvenlik Stratejisi Çalıştayı", "Veri Merkezleri ve Siber Güvenlik Çalıştayı", "Siber Güvenlik Hukuku Çalıştayı", "Mobil Dünyada Çocuk ve Gençlerin Güvenliği Sempozyumu", "IPv6 Konferansı", "Kritik Enerji Altyapılarının Korunması Sempozyumu", "Ulusal Siber Terör Konferansı", "Siber Güvenlik Yaz Kampı" gibi etkinlikleri düzenleyerek ve destekleyerek bilgi güvenliğine ihtiyaç duyulan her alanda çalışmalar yürütmüştür. Cumhurbaşkanlığı, BTK, UAB, MEB, SGK, Üniversiteler gibi farklı paydaşlar ile çalışmalar yürütmektedir.

BGD, CyberMag Dergisi ile toplumun tüm kesimlerine ulaşmaya çalışmaktadır. 2020 yılında 13. sini düzenlediğimiz "Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı" kısaca ISCTurkey Konferansı olarak bilinen uluslararası etkinlik ile kurulduğu günden bu yana kamu kurumları, özel sektör ve üniversiteleri bir araya getirmeyi başarmıştır.

Bununla birlikte, bilgi güvenliği ve siber güvenlik alanında ulusal ve uluslararası düzeyde tarafsız, güvenilir ve etkin bir ulusal sivil toplum kuruluşu olan Bilgi Güvenliği Derneği, bünyesinde oluşturulan BGD Genç ile; bireysel, kurumsal, ulusal ve evrensel boyutlarda bilgi ve iletişim güvenliği alanında teknik, bilimsel, sosyal ve kültürel faaliyetler yürütmek, orta ve yüksek öğrenim gören genç üyelerimizin mesleki gelişimini artırmak, siber güvenlik alanında farkındalık oluşturmak, ülkemizin siber güvenlik uzman kaynağını oluşturmak için gençlerimizin bu alana ilgisini artırmak için faaliyet göstermektedir.

ISCTurkey etkinlikleri, Gazi Üniversitesi, İstanbul Teknik Üniversitesi ve ODTÜ işbirliği ile düzenlenmekte ve Ulaştırma ve Altyapı Bakanlığı, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi ile Bilgi Teknolojileri ve İletişim Kurumu tarafından sürekli desteklenmektedir. Bu etkinlik, Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) tarafından "Avrupa Siber Güvenlik Ayı" platformu etkinliklerine dâhil edilen ilk ve tek etkinliktir. Ayrıca, düzenlendiği ilk yıldan beri ülkemizin siber güvenlik alanındaki bilimsel ve sektörel çalışmaların paylaşıldığı, üniversite-kamu-endüstri işbirliğinin geliştirildiği, kamunun bilgilendirildiği, paydaşların eğitildiği, tüm bilim insanları, araştırmacılar ve sektörel uygulayıcılar arasında bilgi alışverişini sağlayan ülkemizde bu alandaki en önemli etkinliktir.

Bu kitabın hazırlanmasında katkı sağlayan başta editörlerimize, hiç bir beklenti içerisinde olmadan bölüm yazan ve bunu kamuoyu ile ücretsiz paylaşılması konusunda destek veren saygıdeğer yazarlarımıza, sponsorumuza ve bugüne kadar ülke bilgi güvenliği ve siber güvenliğinin gelişimine katkı sağlayan BGD yöneticilerimize ve üyelerimize bu vesile ile şükranlarımı sunarım.

Bu kitap serisinin, ülkemiz siber güvenlik ve savunma çalışmalarına katkılar sağlaması dileğiyle.

Ahmet Hamdi ATALAY

Bilgi Güvenliği Derneği YK Başkanı

EDİTÖRLERDEN

Bilgi Güvenliği Derneği (BGD), kuruluşundan bugüne kadar ülkemizin bilgi ve siber güvenliği ile savunmasının gelişimine katkı sağlamakta, birikimini çevreye aktarmakta, bilgi güvenliği alanında açık kaynak yaklaşımını benimseyen ve bu kapsamda içerik üretilmesine ve geliştirilmesine destek vermekte, bunları yaymakta, paylaşmakta ve kamuoyunun kullanımına sunmaktadır. Düzenlediği ulusal ve uluslararası etkinliklere ait bildiri kitapları serisi, hazırladığı raporlar, taslak strateji dokümanları ve eylem planları vb. bunların başında gelmektedir. Siber Güvenlik ve Savunma Kitapları Serisi ise BGD'nin ülkemizin siber güvenliğine önemli bir katkısıdır.

Tehditlerin, saldırıların veya açıklıkların artması, boyut ve yön değiştirmesi, farklılaşması, siber tehdit ekosisteminin gittikçe güçlenmeye başlaması, kritik altyapıların hedef haline gelmesi, bilgi ve kaynak hırsızlıklarının çoğalması, yeraltı yapıların etkinleşmesi, siber tehditlerin artık savaşa dönüşmesi, siber suç ve suçlularının çoğalması, siber terörün yaygınlaşması vb. olumsuzlukların hızla artması, yapılacak mücadele, alınacak önlem ve karşı koyulacak yaklaşımlara duyulan ihtiyacı artırmıştır. Kapsamlı bir mücadele için; ulusal strateji ve eylem planlarına, araştırma merkezlerine, gelişmiş altyapı ve araçlara, lisans ve lisansüstü programlara, nitelikli insan kaynağına, yerli ve milli ürünlerin geliştirilmesine, siber güvenlik ve savunma ekosisteminin oluşturulmasına, ulusal siber olaylara müdahale ekiplerinin sayısının ve niteliğinin arttırılmasına, savunma sanayinin gelişmesine katkı sağlayacak yeni çalışma ve projelerin hayata geçirilmesine mevcut sistem, yapı ve organizasyonların kapsamının büyütülmesine, yeni yapıların kurulmasına ihtiyaç vardır. Duyulan bu ihtiyacı bir nebze de olsa karşılamak için bu kitap serisi hazırlanmıştır. Bu kitap serisinde, 100'e yakın konu başlığı irdelenmektedir. Her bölümde, farklı bir konu siber güvenlik ve savunma kapsamında ele alınmakta, değerlendirilmekte ve alınması gereken önlemlere yer verilmektedir.

Bu kitap serisinde sunulan konu başlıkları, ülkemizde bu alanda çalışan akademisyenler, uzmanlar ve çalışanlar ile paylaşılmış ve bu kitap serisine katkı sağlamaları istenilmiştir. Zamanı uygun olan, katkı vermek isteyen uzman veya akademisyenler belirlenen bir konuda bölüm yazarı olmaları için davet edilmişlerdir. Belirlenen süre içerisinde bölümlerini tamamlayan yazarlarımızın eserleri ise uygun olan ciltlerde basılmaktadır. Bundan sonraki süreçte, belirlenen diğer konular belirli sürelerde tamamlanıp takip eden ciltlerde yayımlanacaktır. Siber güvenlik ve savunmaya çok kapsamlı bir bakış sunmayı amaçlayan ve farklı başlıkları bir araya toplayan bu kapsamlı eserin, ülke siber güvenliğimiz ve savunmasına katkı sağlaması beklenmektedir.

Bu kitap serimizin dördüncü cildinde, 15 farklı bölüm sunulmuştur. Siber güvenliğin farklı açılardan irdelendiği bu ciltte; siber güvenliğin kapsamı ve boyutu, yapılan saldırıların türleri, alınabilecek önlemler, karşılaşılan yeni riskler ve problemlere yer verilmiş, karşılaşılabilecek risklere dikkat çekilmiş ve sonuçta alınması gereken önlemler ve yapılması gerekenler özetlenmiştir. Her bir bölüm; ülkemizde bu alana katkı sağlayan, bu alanda eğitim almış, tez hazırlamış, çalışmalar yapmış değerli akademisyen, kamu çalışanı ve üst düzey yöneticiler tarafından hazırlanmıştır. Her bir bölüm, birbirinden bağımsız olarak hazırlansa da konu bütünlüğü ve devamlılığının sağlanmasına mümkün olduğunca dikkat edilmiştir. Her bölüm tarafımızdan değerlendirilmiş, yazarlara konu içeriği ve başlıklarla ilgili olarak bazı önerilerde bulunulmuş, düzeltmeler yapılması istenilmiş ve sonuçta yapılan değişiklikler dikkate alınarak bu kitap hazırlanmıştır. Kitapta yazılan bölümler intihal taramasından geçirilmiş, tekrar tekrar kontrol edilmiş, yapılan çalışmalar ise her bölümün sonunda bölüm yazarları tarafından değerlendirilmiştir.

Bu kitabın, siber güvenlik ve savunma konusunda yapılacak çalışmalara ışık tutması, yeni çalışmaların yapılmasına katkı sağlaması, bu konuda yapılacak olan işbirliklerini geliştirmesi, bu konunun boyutunun ve kapsamının daha iyi anlaşılmasına katkı sağlaması ve en önemlisi ise bilgi güvenliği ve siber güvenlik alanında duyulan ihtiyacı bir nebze de olsa karşılaması, açık kaynak olarak sunulması ile de kaynaklara erişimi kolaylaştırıcı bir başvuru kitabı serisi olması beklenmektedir. Bu eser serisi açık kaynak olarak, Bilgi Güvenliği Derneği web sayfasında (www.bilgiguvenligi.org.tr) yayımlanmaktadır.

Bu kitapta yazarlarımız; alan uzmanlıklarına göre bölümleri hazırlamışlar, kişisel ve kurumsal bilgi birikimlerini hazırladıkları bölümlerde sunmuşlar, hazırladıkları bölümlerin açık kaynak olarak yayımlanmasını kabul etmişler ve bu kitabın basımı ve dağıtımı ile ilgili olarak herhangi bir telif hakkı talep etmemişlerdir. Yazarlarımıza, bu kitap serisinin editörleri olarak çok özel teşekkürlerimi ve şükranlarımı sunarız.

Kitabın titizlikle hazırlanmasında, kontrolünde ve basılmasında başta yazarlarımız olmak üzere emeği geçen tüm paydaşlarımıza, bu fikri hayata geçiren Bilgi Güvenliği Derneği YK üyelerimize ve özellikle de basılmasına maddi destek veren HAVELSAN A.Ş.'ye teşekkürlerimizi sunarız.

Prof. Dr. Şeref SAĞIROĞLU
BGD Kurucu Üyesi ve II. Başkanı
Gazi Üniversitesi Mühendislik Fakültesi Dekanı
FutureTech Genel Müdürü

Doç. Dr. Sedat AKLEYLEK
BGD Ulusal Bilim Kurulu Üyesi,
Ondokuz Mayıs Üniversitesi Mühendislik Fakültesi
Bilgisayar Mühendisliği Bölümü Öğretim Üyesi
SdataM Bilişim Teknolojileri ve Güvenliği
Ltd. Şti. Kurucu Ortağı

İÇİNDEKİLER

Bölüm 1

SİS BİLİŞİMİ VE UYGULAMALARINDA VERİ GÜVENLİĞİ

Sedat Akleylek - Aykut Karakaya

Kitabımızın bu bölümünde, sis bilgi işlem platformunun özellikleri, bulut ve kenar bilgi işlem platformları ile karşılaştırılması, sis ağının güvenlik ihtiyaçları incelenmiş, nesnelerin interneti (IoT) uygulamalarındaki kullanımı ve etkileri gözden geçirilmiş, IoT uygulamalarını daha verimli ve performanslı hale getirmek için kullanılan bulut (cloud), sis (fog) ve kenar (edge) bilgi işlem yapılarının farkı ortaya konmuştur. IoT uygulamalarında bant genişliği, hız, güvenlik gibi özelliklerin verimliliği noktasında hangi yapının kullanılmasının daha avantajlı olacağı gösterilmiştir. Ayrıca, bulut, sis ve kenar bilgi işlem sistemlerinin karşılaştığı güvenlik sorunları detaylı bir şekilde incelenmiştir. Ayrıca, bu bölümde verilen karşılaştırma tabloları ve sistem şemalarına göre IoT uygulamalarında kullanılabilecek yapılar ve karşılaşılabilecek sorunlar değerlendirilmektedir. Bu kapsamda IoT uygulamaları geliştirilebilir ve sis, bulut, kenar sistemlerinde karşılaşılan sorunlara çözüm aranabilir.

Gelişmekte olan sis bilişim yapısında güvenlik en önemli noktalardan biridir. Veriler bulut sunucuya gitmeden önce sis düğümlerinde işlendiği için sis katmanının güvenliği sağlanmak zorundadır. Sis güvenliği için yapılan çalışmalar ve sis düğümlerinin maruz kaldığı saldırı türleri incelenmiş, sis düğümlerine yapılan olası tüm saldırıları engelleyen bir model geliştirmek zor olduğu için buna benzer bir modelin geliştirilebilmesi için yönlendirmeler ve önerilerde bulunulmuştur.

Sonuç olarak; sis bilgi işlem platformunun özellikleri, güvenlik ve gizlilik durumları, IoT uygulamalarındaki yeri, sis bilişimin özellikleri, bulut, kenar ve sis bilgi işlem yapılarının karşılaştırılması, IoT ile sis bilişim kullanımında güvenlik ihtiyaçları ve IoT uygulamalarına sis bilişim yapılarının dâhil edilmesi için kullanılan ortamlar bu bölüme dâhil edilmiş ve elde edilen sonuçların değerlendirilmesine yer verilmiştir.

1.1. GİRİŞ

Nesnelerin İnterneti (Internet of Things - IoT), akıllı tanıma, izleme, yönetim işlerini yürütmek için algılayıcı ekipmanlar ile belirlenen protokollere bağlı olarak gerçekleşen ve bir nesneyi İnternete bağlayan veya yerel ağda haberleştiren bir ağ türüdür [1]. Akıllı endüstri, akıllı ev sistemleri, akıllı şehir, sağlık, askerî, tarım, eğitim, araç sistemleri vb. çok çeşitli alanlarda uygulamaları bulunmaktadır. Bir IoT sistemin genel yapısı Şekil 1.1'de gösterilmektedir.

Şekil 1.1. IoT sistemlerin genel yapısı

Sis bilişim (fog computing), çok büyük ölçekli IoT uygulamalarını desteklemek için depolama, bilgi işlem ve ağ kaynaklarını ağ kenarında doğru genişleten bulut bilişimde yeni bir merkezi olmayan mimaridir. Bulut, sis ve kenar bilişim sistemleri IoT uygulamalarına hesaplama, depolama, uygulama, altyapı ve veri kaynakları sağlamaktadır. Aralarında bazı önemli farklar vardır. En büyük fark, erişilebilirlik ve yakınlıktır. Sis ve kenar bilişimde veri merkezleri, sistemdeki düğümlere yakındır ve genellikle yerel ağda bulunmaktadır. Bulut ise dünyanın herhangi bir yerinde internet üzerinden

erişilen sunucu veya veri merkezidir. Sis, çeşitli hizmetler için gerekli olan sanal sensörleri ve ağları oluşturmak için sanallaştırmayı kullanarak bulutu genişletmektedir. Bir başka deyişle, düğümlerle bulut arasında bir katman gibidir. Veri analizine, veri işlemeye ve filtrelemeye yardımcı olmakta ve hassas veriler için güvenliği arttırmaktadır. Kaynak kısıtlı ve birbirine yakın mesafede çalışan cihazlarda depolama ve hesaplama gibi işlemlerde sis buluttan daha etkilidir. Bulut daha merkezî iken sis dağıtılmış uygulamalarda daha iyidir.

Sis bilişim sistemleri çok sayıda avantaja sahiptir. Ağın daha küçük kapsamda olmasından dolayı düşük gecikmeli, enerji tasarruflu ve yüksek güvenlikli iletim yapılması en önemli avantajları arasında sayılabilir. Geleneksel ağ güvenliğinde olduğu gibi IoT uygulamalarındaki sis bilişim güvenliğinde de amaç; gizlilik, veri bütünlüğü, erişilebilirlik, güvenilirlik, kimlik doğrulama gibi ilkelerin sağlanmasıdır. Sis Bilişim, uç cihazlar ile uzaktaki bulut veri merkezleri arasında bilgi işleme ve depolama gibi hizmetleri sağlayan yerel ve sanallaştırılmış bir platformdur [2]. Sis bilişim ile IoT uygulamaları daha verimli ve daha güvenli hâle gelmektedir. IoT uygulamalarında kaynak kısıtlı algılayıcılar (sensörler) kullanılmaktadır. Algılayıcılar aracılığıyla toplanan verilerin işlenmesi, depolanması, şifrelenmesi gibi büyük hesaplama gerektiren işlemler için kaynak kapasitesi yüksek olan cihazlara ihtiyaç duyulmaktadır. Bu işlemler kaynak kısıtlı olan algılayıcılar tarafından yapılamamaktadır. Genellikle uzaktaki sunucu olarak hizmet veren bulut düğümlerinden, yerel olarak hizmet veren sis düğümlerinden veya kenar bilişimde olduğu gibi uç mobil cihazlardan yararlanılmaktadır. Her bilişim sisteminin kendine özgü bazı avantaj ve dezavantajları vardır ve ilerleyen bölümlerde ayrıntılı olarak ele alınmaktadır.

IoT uygulamalarında uç cihazlar olarak kullanılan algılayıcılara yakın yerde yerel bir çözüm olarak sis ağı (fog net) kurulabilmektedir. Sis bilişim algılayıcılardan elde edilen verilerin buluta gönderilmeden işlenebilmesi, depolanması ve korunması için etkili bir yöntemdir. Buluta veriler gönderilirken güvenli olmayan internet ağı kullanılmaktadır. IoT cihazlarının algılanan verileri doğrudan (sis ağı kullanmadan) buluta göndermesi verilerin çalınması, değiştirilmesi gibi riskler taşımaktadır. Ayrıca verilerin işlenmesi ve depolanması fazla zaman almakta ve uç cihazlara dönen yanıtın gecikme süresi artmaktadır. Sis bilişim kullanıldığında ise veriler yerel olarak işlendiği için

uç birimlere dönen yanıtın gecikme süresi azalmaktadır. Ayrıca verilerin işlendikten sonra kalıcı depolanmak üzere buluta gönderilmesi gerekiyorsa, veriler güvenli olmayan internet ağı üzerinden geçerken şifreleme işlemleri ile koruma altına alınabilmektedir.

Sistemin performansını arttırmak için IoT uygulamalarında sis bilişim kullanmak gerekmektedir. Gecikmenin az olması istenen arttırılmış gerçeklik, içerik dağıtımı ve önbellekleme, mobil büyük veri analizi, akıllı şebekeler, akıllı ev sistemleri, akıllı trafik izleme, akıllı sağlık sistemleri gibi birçok uygulamada sis kullanılmalıdır [2].

Sis bilişim büyük miktarda IoT verisini buluta göndermek yerine yereldeki düğümler ile verileri işlemektedir. Milisaniyeler içinde verilerin analizini yaparak uç cihazlara yanıt dönmektedir. Daha uzun süreli depolama ve tarihsel analiz durumunda verileri buluta göndermektedir [3]. IoT uygulamaları için veri işlemede gecikmenin az olması oldukça önemlidir. Örneğin; bir fabrikada, kimyasal maddenin ısıtıldığı bir kazanda sıcaklık artışını izleyen sensörler ile iş süreçleri takip edilebilmekte veya benzer şekilde bir hastanede, hastalara yerleştirilen nabız, vücut ısısı, EKG gibi sensörler ile hastaların durumları takip edilebilmektedir. Buna benzer, hızlı tepkiler alınmasının hayati öneme sahip olduğu IoT uygulamalarında sis bilişim sistemleri yüksek performans, düşük gecikme ve enerji tasarrufu sağlamaktadır.

İnternete bağlanan nesnelerin sayısının artması ile günlük üretilen veri miktarı da hızla artmaktadır. Bütün bu verileri buluta aktarmak yüksek miktarda bant genişliği gerektirmektedir. Bu yüzden bazı verilerin yerel ortamdaki sis ağında analiz edilmesi ve sadece uzun süreli depolanması gereken verilen buluta gönderilmesi bant genişliğini azaltmaktadır [3]. Kısaca özetlemek gerekirse; IoT uygulamalarında yerel bir çözüm olan sis bilişimin kullanılması, gecikmeyi en aza indirmekte, ağ bant genişliği tasarrufu sağlamakta, internet ortamından kaynaklanan güvenlik sorunlarını gidermeye destek sağlamaktadır.

Sis ağının kurulması, ölçeklendirilebilmesi, veriminin arttırılması ve maliyetinin azaltılması için Yazılımla Tanımlanan Ağ (Software Defined Network - SDN) ve Ağ İşlevi Sanallaştırması (Network Functions Virtualization - NFV) tabanlı yapılardan yararlanılmaktadır. SDN, küresel ağın daha akıllı, soyut ve işlevsel olmasını sağlayan yazılım tabanlı olarak gerçekleştirilen teknolojiler,

modeller ve protokolleri kapsamaktadır. NFV ise ağ işlevlerini sanallaştırmak, ağ entegrasyonunu arttırmak için geliştirilen yüksek hacimli yapıları kapsamaktadır. Her bir IoT bileşenini birbirine bağlayan sis ağlarında yönetim ve sürdürülebilir bağlantı elde etmek zordur. Kolay yönetim, ölçeklenebilirlik gibi sistemin verimini arttıran işlemler için SDN ve NFV teknikleri kullanılmaktadır [4]. Her bir sis düğümünün multi-hop (çok atlamalı - düğümden düğüme) iletişim kurabilmesi gerekmektedir. Bu nedenle her düğüm sis ağı içinde yönlendirici görevi görmektedir. IoT platformunda sis düğümlerinin etkin yönlendirme yapabilmesi için son yıllarda hiyerarşik SDN tabanlı sis mimarisi üzerine çalışmalar artmaktadır [5]. NFV, sanallaştırma ile yazılımı donanımdan ayırarak ağ işlevlerinin daha hızlı gerçekleşmesini sağlamaktadır. Bu nedenle son yıllarda NFV tabanlı hibrit bulut ve sis sistemleri geliştirilerek ağın maliyetini en aza indirmek için çalışmalar yapılmaktadır [6].

SDN ve NFV tabanlı yaklaşımlar sis ağının performansını ve servis kalitesini arttırmaktadır. Sis ağlarının servis kalitesini belirlemek için önemli ölçümler yapılmaktadır. Bunlar bağlantı, güvenilirlik, kapasite ve gecikme ölçümleridir. Bağlantı ölçümünde ağın hızlı ve güvenilir olması beklenmektedir. Güvenilirlik ölçümünde, verilerin doğru ve eksiksiz iletilmesi beklenmektedir. Ancak bunu gerçekleştirmek için veriler bir takım kontrol (veri bütünlüğünün sağlanması) işlemlerinden geçirilmelidir [7]. Bu da sisteme ek gecikme yükü getirmektedir. Kapasite ölçümünde, ağın bant genişliği ve depolama alanlarını verimli kullanması beklenmektedir. Bu yüzden önce veri toplanır, sonra hesaplama gerçekleşir. Böylece önbellek farklı işler için yeniden tasarlanabilir [8]. Bu işlem de gecikmeye neden olmaktadır. Gecikme ölçümünde ise düğümlerin hesaplama ve depolama işlemlerinden hızlı yanıt alması beklenmektedir. Akış madenciliği, karmaşık olay işleme gibi teknikler gelecek işlemleri öngörerek gecikmeyi azaltabilir.

IoT geliştiricilerinin uygulamalarını sis bilişim platformuna taşımalarını kolaylaştırmak için arayüz ve programlama modellerine ihtiyaç vardır. Ortamdaki bileşenlerin farklı platformlara uyum sağlayabilmesi için dinamik, hiyerarşik kaynakların buna göre optimize edilmesi gerekmektedir [4]. IoT uygulamalarında uç düğümler hareketli olabilmektedir. Kaynak yönetimi durumunda uç düğümün hareketli olması zorluklar oluşturmaktadır. Çünkü bant genişliği, depolama, hesaplama, gecikme durumları dinamik olarak değişmektedir. Kaynak yönetimi ve paylaşımı için CPU, bant genişliği, depolama

gibi heterojen kaynakları sis düğümlerine uygun şekilde paylaştıran yapılar üzerine çalışmalar yapılmaktadır [9].

Sis, kenar ve bulut bilişim birbirlerine benzer veri merkezleri olmasına rağmen bazı temel farklılıkları bulunmaktadır. Sis bilişim, bulut ve kullanıcılar arasında bir ara katman gibi çalışmakta, kaynak kısıtlı cihazlardan aldıkları verileri yerel ağda işleyerek gecikmesi düşük yanıtlar üretmektedir. Kenar bilişimde, veriler kaynak kısıtlı uç düğümlerde işlenmektedir. Bulut bilişimde ise veriler kaynak kısıtlı cihazlardan doğrudan uzaktaki bulut sunucularına gönderilmektedir. Sis bilişimin kenar bilişime göre avantajı, veri işlemeyi yüksek işlem kapasitesine sahip cihazlarda hızlı bir şekilde yapabilmesi ve depolama kapasitesinin yüksek olması iken bulut bilişime göre avantajı, düşük gecikme, enerji tasarrufu ve verilerin güvensiz olan internet ortamına çıkmadan işlenebilmesidir. Veriler buluta gönderilirken veya işlenmek için beklerken şifreli olarak tutulmaktadır. Bu sayede sis katmanı IoT ağını uç sistemlere doğru genişletirken güvenlik düzeyini arttırmaktadır. Ancak doğrudan sis sunucularına yapılan saldırılar (solucan deliği, kimlik kopyalama vb.) da bulunmaktadır. Bu saldırıları önlemek için sis bilişime uygun güvenli modeller geliştirilmektedir.

Sis ağının güvenliğinin sağlanması için kimlik doğrulama, erişim kontrolü, saldırı tespiti, gizlilik şemaları gibi modeller geliştirilmektedir. Sis bilişim IoT sistemlerine bir sis servis sağlayıcısı aracılığıyla hizmet vermektedir. Çok sayıda sis servis sağlayıcı kurum olduğu için sis düğümleri de güvenlik ve gizlilik tehditleriyle karşı karşıya kalmaktadır [10]. Bir başka deyişle, servis sağlayıcı hizmeti veren kurumun güvenilir olmaması durumunda sis düğümleri saldırılara karşı savunmasız olmaktadır.

Sis sunucularına yapılan saldırılardan dolayı sis bilişimde birtakım güvenlik ihtiyaçları bulunmaktadır. Bu güvenlik ihtiyaçları; sis düğümlerinin ve kullanıcı cihazlarının kimliklerinin doğrulanması, verilerin korunması ve gizlenmesi, verilerin doğruluğunun ve bütünlüğünün sağlanması, kötü amaçlı düğümlerin tespit edilmesi, yetkili düğümler tarafından sistemden kesintisiz hizmet alınabilmesi, hesaplama maliyetinin düşürülmesi, farklı protokoldeki cihazların birbirleriyle sorunsuz haberleşebilmesi, ağ tıkanıklıklarının önlenmesi, şifreleme işlemlerinde anahtar yönetiminin güvenli ve verimli bir şekilde yapılabilmesidir.

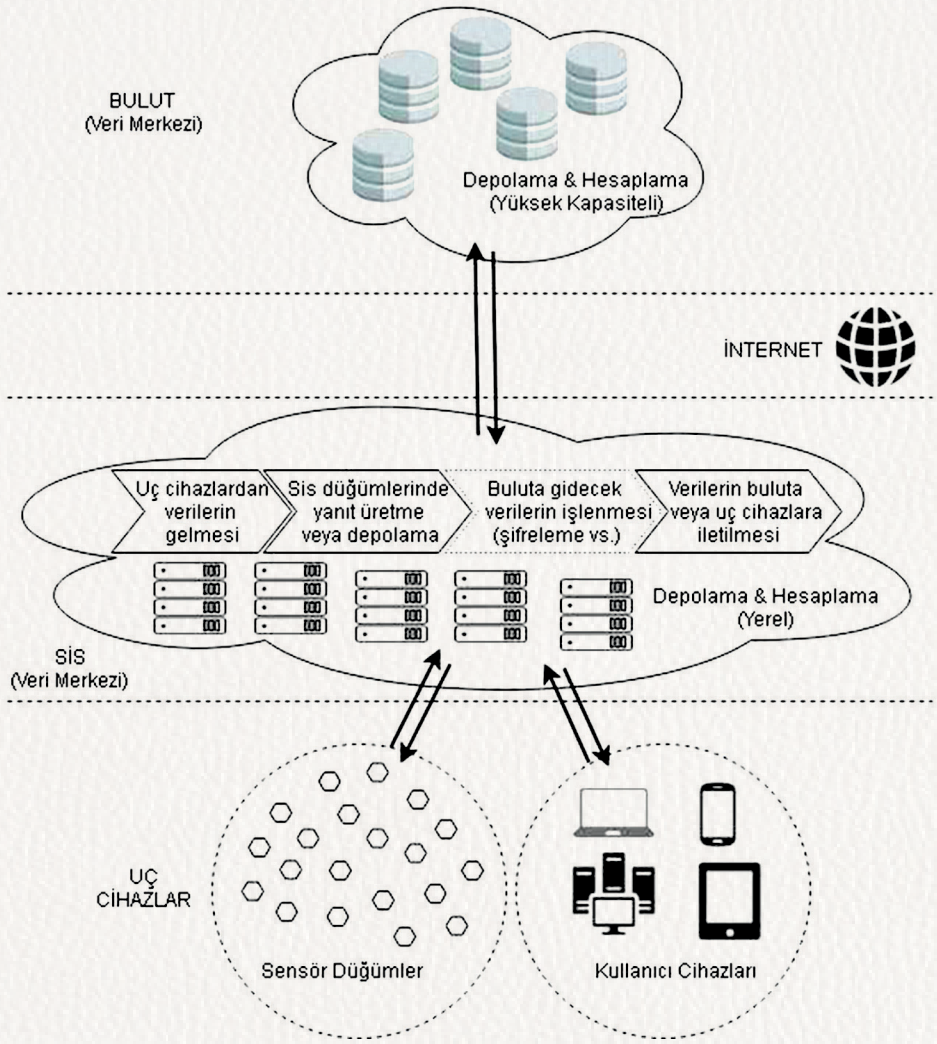
1.2. SİS BİLİŞİMİN ÖZELLİKLERİ

Sis bilişim, yerel ortamda verilerin işlenmesi, depolanması ve taşınması işlemlerini gerçekleştirmektedir. Bulut bilişimin yapısı gereği çözülemeyen sorunları sis bilişim esnek kaynaklar ve hizmetler sunarak çözebilir. Bu sorunlar; neden olduğu bilinmeyen güvensiz iletim gecikmesi, hareketli düğüm desteği eksikliği, yüksek bant genişliği ve konum farkındalığıdır. Sis bilişimde ağın kenarındaki servisler sis düğümleri tarafından sağlanmaktadır.

Sis bilişim özellikleri [2];

- Düşük gecikme süresi: Uzaktaki bulut ağı yerine yereldeki sis ağında veriler işlenmekte ve depolanmaktadır. Bu yüzden uç düğümler sis ağında işlenen verilerin yanıtını daha düşük gecikme ile almaktadır.
- Geniş coğrafi dağılım: Sis bilişim IoT uygulamalarının performansını önemli ölçüde arttırdığı için akıllı şebeke gibi IoT uygulamalarında geniş bir coğrafi alanda hizmet verebilmektedir.
- Konum farkındalığı: Sis düğümleri ağın kenarında bulunan servisleriyle uç düğümlerin yerini bulabilmektedir. Hareketli uç düğümlerin de ağa dâhil olabilmesini sağlamaktadır.
- Çok sayıda düğüm: Akıllı şehir, akıllı şebeke gibi IoT uygulamalarında sis bilişim kullanılabilmektedir. Bu IoT uygulamaları çok sayıda uç düğüm barındırmaktadır. Ayrıca uygulama yapısında sis görevi gören düğümler de sayıca fazla olabilmektedir.
- Gerçek zamanlı uygulamalar: Sis bilişim düşük gecikmeye sahip olduğu için güçlü veri akışı sağlamaktadır. Bu yüzden gerçek zamanlı uygulamaların performansını arttırmaktadır.
- Heterojenlik: Sis bilişim ve sis düğümleri, farklı aygıtın veya farklı servislerin birlikte çalışabilmesini sağlamaktadır. Sis ağı geniş coğrafi alana yayılabildiği için sistemde birçok farklı aktör olabilmektedir.
- Güvenlik: Bulut bilişim kullanan bir IoT uygulamasında sis düğümleri kaynak kısıtlı uç cihazların yapamadığı hesaplama, şifreleme gibi işlemleri gerçekleştirebilmektedir. Böylece veriler güvensiz olan internet ortamından geçerken korunabilmektedir.

Sis bilişim, IoT uygulamalarında uç cihazlardan aldığı verileri işleyebilir, depolayabilir veya buluta iletebilir. Bu nedenle sis ağı IoT uç cihazları ile uzaktaki bulut sunucuları arasında bir ara katman görevi görmektedir.



Şekil 1.2. Sis bilişimde verilerin işlenmesi, depolanması ve taşınması

Sis bilişimde en yaygın kullanılan mimari yapısı 3 katmanlı mimaridir. 1. katman, algılayıcı düğümler, akıllı cihazlar, IoT özellikli cihazlar gibi uç cihazlardan oluşur. Uç cihazlar Global Konumlandırma Sistemi (Global Positioning System - GPS) ile donatılmıştır. 2. katman, yönlendirici, ağ geçidi, anahtar (switch), erişim noktaları, sunucu sistemler gibi sis düğümlerinden

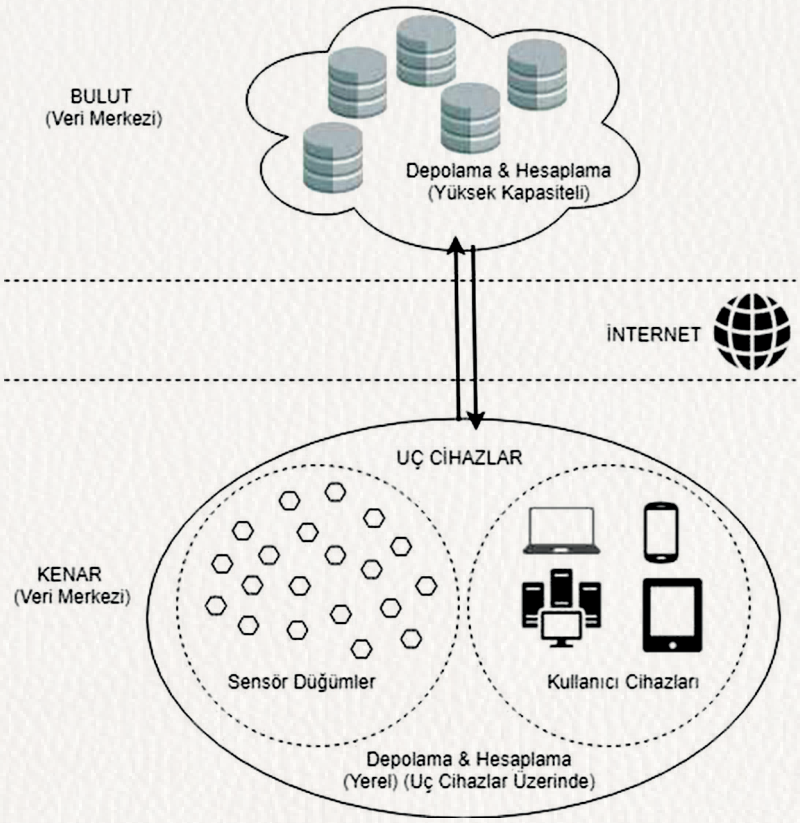
oluşur. Sis düğümleri veri depolama, iletim, bilgi işleme faaliyetlerini yürütür. 3. katman ise, uzaktaki bulut sunucularından oluşur. Yeterli derecede depolama ve bilgi işleme hizmeti sunar [11]. Kaynakları kısıtlı olan uç cihazların elde ettikleri veriler sis düğümleri tarafından işlenerek buluta veya uç cihaza yanıt olarak geri gönderilmektedir. Uç cihazlara yanıtlar yerel ağdan gönderildiği için gecikme düşüktür ve buluta iletilen veriler korunabilir. Sis bilişimde verilerin işlenmesi, depolanması ve taşınması Şekil 1.2'de gösterilmektedir.

1.3. SİS, KENAR VE BULUT BİLİŞİM

Sis bilişim ve kenar bilişim veri işlenmesi ve depolanmasına yerel bir çözüm oluşturmaktadır. Bulut bilişim ise internet üzerinden erişilen uzaktaki düğüm ile gerçekleşmektedir. Sis bilişim son kullanıcılara servis gecikmesini azaltır. Bulut bilişimin sunduğu depolama, ağ oluşturma, bilgi işleme olanaklarını ağın kenarına doğru genişletmektedir. Bu nedenle sis bilgi işlem yöntemi sistemin performansını ve verimini arttıran bir bileşendir [12]. Bulut bilişim uzaktaki sunucu aracılığıyla verileri optimize ederken sis ve kenar bilişim yerel ortamı optimize etmekte ve yönetmektedir. Sis düşük gecikme süresi, güvenlik adımları oluşturma, konum farkındalığı, yerel olma vb. özelliklere sahip iken kenar bilişim kısa mesafeden dolayı güvenli, kaynak kısıtlı, düşük hesaplama kapasitesi, yerel olma vb. özelliklere sahiptir. Bulut ise yüksek gecikme süresi, güvenlik adımları tanımlı olmayan, konum farkındalığı bulunmayan, küresel olma vb. özelliklere sahiptir.

Kenar ile sis bilişim her ikisi de veri yönetimine yerel çözümler getirmektedir. Fark olarak; kenar bilişim işini uç cihazlar olan sensörler, mobil cihazlar üzerinde yapmaktadır [13]. Sis bilişim ise hesaplama işini sis düğümlerinde gerçekleştirerek verileri buluta veya uç cihazlara yanıt olarak göndermektedir. Kenar tamamen yerelleştirilmiştir. Sis ise hesaplama ve iletişim kaynaklarını ağın kenarlarına doğru genişletmektedir [11]. Başka bir deyişle, sis uç cihazlar ile uzun süreli depolama görevi gören bulut sistemleri arasında bir katmandır. Kenar bilişimde verilerin işlenmesi, depolanması ve taşınması Şekil 1.3'te gösterilmektedir.

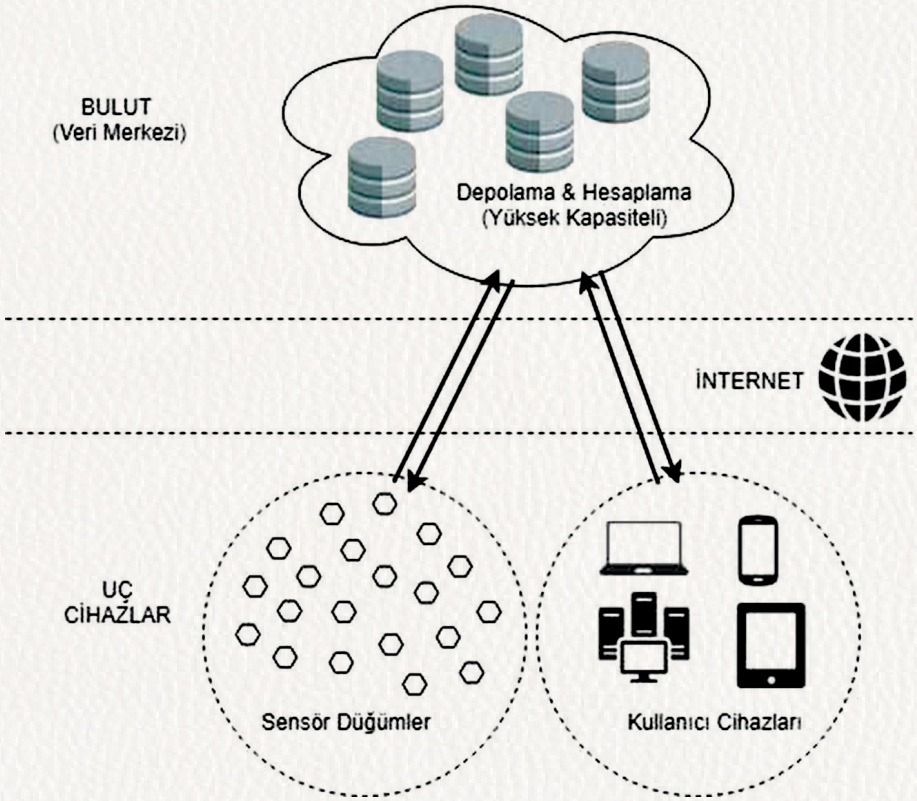
Kenar bilişim bulut servislerini doğrudan desteklemediği için gerçek zamanlı veri işleme adımı ile veriler işlenerek buluta gönderilmektedir.



Şekil 1.3. Kenar bilişimde verilerin işlenmesi, depolanması ve taşınması

Veri merkezleri konusunda son dönemlerde oldukça popülerleşen Çoklu Erişim Kenar Bilişim (Multi-Access Edge Computing) sistemleri bulut hizmetlerini ağın kenarına doğru genişleterek baz istasyonları aracılığıyla verilerin depolanması ve işlenmesi için kaynak sağlamaktadır. Bu yönüyle sis bilişim sistemlerine oldukça benzeyen MEC yapısı kenar bilişim sistemlerinin performansını arttırmaktadır. MEC yapısı sis bilişime benzer olarak heterojen kaynaklara hizmet edebilme, sanallaştırma, mobilite, düşük gecikme ve ölçeklenebilirlik desteği sunmaktadır [14]. Fark olarak ise telekom şirketleri tarafından hizmet alınması ve uç sistemlere daha yakın olduğu için daha hızlı olması gibi özellikleri bulunmaktadır. Sis bilişimin MEC yapısına göre en önemli avantajı ise Telekom şirketlerinden bağımsız özel ağlar kurulabilmesidir.

Bulut bilişimde ise algılayıcı uç cihazlardan elde edilen veriler depolama ve veri işleme için doğrudan buluta gönderilmektedir. Veriler ilk hâli ile internet ortamından geçirilerek buluta gönderildiği için veri güvenlik zafiyetleri oluşturmaktadır. Veri güvenliği uç cihazlar üzerinde yapılabilmektedir. Fakat kaynak kısıtlı cihazlarda şifreleme ve koruma gibi hesaplama işlerinin maliyeti yüksektir. Bulut bilişimde verilerin işlenmesi, depolanması ve taşınması Şekil 1.4'te gösterilmektedir.



Şekil 1.4. Bulut bilişimde verilerin işlenmesi, depolanması ve taşınması

Sis veya kenar bilişim sistemlerini kullanan IoT modelleri tasarlanırken genellikle bulut sistemler de tasarıma entegre edilmektedir. Bulut, kenar ve sis bilişim arasındaki karşılaştırma bilgisi Tablo 1.1'de gösterilmektedir.

Tablo 1.1. Bulut, sis ve kenar bilişim karşılaştırması

Bulut Bilişim	Sis Bilişim	Kenar Bilişim
Gecikme yüksek	Gecikme düşük	Gecikme yüksek
Yanıt süresi uzun	Yanıt süresi kısa	Yanıt süresi uzun
Veri işleme ve depolama işlemi: İnternet üzerinden erişilen cihazda	Veri işleme ve depolama işlemi: Sis katmandaki cihazlarda	Veri işleme ve depolama işlemi: Uç cihazlarda
İnternet bağlantılı	Yerel	Yerel
Depolama ve veri işleme kapasitesi: Yüksek	Depolama ve veri işleme kapasitesi: Yüksek	Depolama ve veri işleme kapasitesi: Düşük
Merkezî işlem	Dağıtık işlem	Dağıtık işlem

Bulut, sis ve kenar bilişimde hesaplama işlemlerinin hepsinde bir takım güvenlik tehditleri bulunmaktadır. Bu tehditlerin bazıları üçü için de ortak iken bazıları birini veya ikisini ilgilendirmektedir. Bulut, sis ve kenar bilişim sistemlerinin karşılaştığı tehditler Tablo 1.2'de gösterilmektedir.

Tablo 1.2. Bulut, sis ve kenar bilişimin karşılaştığı güvenlik tehditleri

Güvenlik Tehditleri	Etkilediği Bilişim Sistemi
Fiziksel Saldırılar	Bulut (uç cihazlara), Sis (sis düğümlerine ve uç cihazlara), Kenar (uç cihazlara)
Hizmet Reddi (DoS), (XML-DoS ve HTTP- DoS)	Bulut, Kenar, Sis (kötü niyetli düğümler ile)
Aradaki Kişi (Man In The Middle)	Bulut (İnternet ortamında – IP, DNS vs. sızması ile), Kenar ve Sis (yerel ağa sızma ile)
Sybil Saldırısı (sensörlerin kimliğini kopyalama)	Bulut, Kenar, Sis (IoT uygulamalarında kullanıldıklarında)
Wormhole Saldırısı (sensör düğümler içinde kısa yollar oluşturma)	Bulut, Kenar, Sis (IoT uygulamalarında kullanıldıklarında)
Kötücül Yazılım Enjeksiyonu (Malware Injection)	Bulut, Kenar, Sis
Şifreleme Sistemlerine Saldırılar	Kenar (kaynak kısıtlı uç cihazlar ile şifreleme yapılır.), Sis (sis ağındaki düğümler ile şifreleme yapılır.)
Sanal Makine Saldırıları	Bulut, Kenar ve Sis (altyapılara yapılan)
Kötü Tasarlanmış Altyapılar, Güvensiz Servis Sağlayıcılar, Kablosuz Ağ Sorunları gibi durumlar kullanılarak yapılan saldırılar	Bulut, Kenar ve Sis

IoT uygulamalarında bulut, kenar ve sis bilişim Tablo 1.2'de de görüldüğü gibi genellikle benzer tehditler ile karşı karşıya kalmaktadır. Bulut bilişimin internet ortamında olması, kenar ve sis bilişimin yerel olması bu saldırıların uygulanma biçimi arasında farklılıklar meydana getirmektedir.

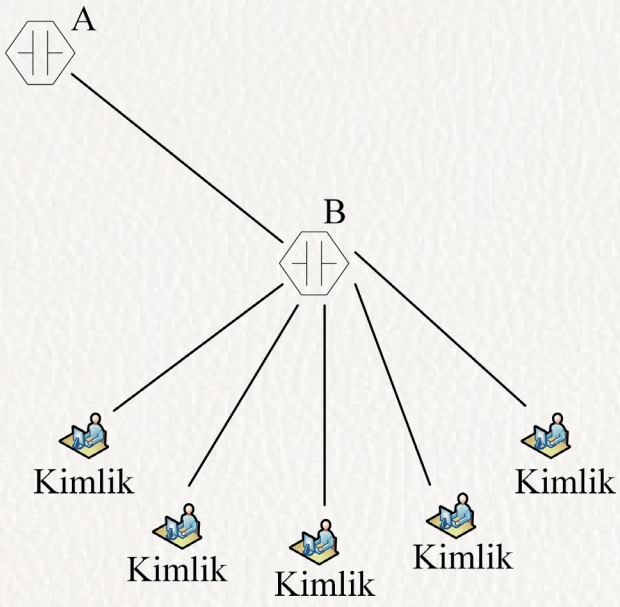
IoT sistemlerin uç cihazları bir veya birkaç sensörden oluşan modeller olabilmesinin yanı sıra Kablosuz Sensör Ağları (Wireless Sensor Networks - WSN), Kablosuz Vücut Alan Ağları (Wireless Body Area Networks -WBAN) gibi çok sayıda sensörün birbirleriyle etkileşimli çalıştığı yöntemler de kullanılabilmektedir. Bu sensörler çok atlamalı (multi-hop) bağlantı içermektedir. Çok atlamalı bağlantı verinin algılandıktan sonra veri merkezine gelene kadar düğümler arasında iletilmesi şeklinde gerçekleşmektedir.

Bir veri, merkeze gidene kadar çok sayıda düğümden geçtiği için bazı saldırılara maruz kalabilmektedir. IoT sistemlerini ve dolayısıyla çok sensörden oluşabilen sis bilişim yapısını da etkileyen bu tarz saldırılar Kimlik Kopyalama (Sybil) ve Solucan Deliği (Wormhole) saldırılarıdır.

1.3.1. Sybil Saldırısı

Bir düğüme birkaç tane kimlik tanınmasından oluşan saldırıdır. Böylece bir düşman aynı anda çeşitli yerlerde olabilir. Hataya dayanıklı sistemlerin etkinliğini ciddi ölçüde azaltır [15]. Bir düğüme birkaç tane kimlik atanabildiği için lokasyon bilgisi değiştirilebilir.

Dağıtık depolama, dağılma ve çok yollu yönlendirme, topoloji bakımı gibi hataya dayanıklı şemaların verimli çalışmasını azaltır. Sybil saldırısı Şekil 1.5'te gösterilmektedir. Şekilde saldırgan olan B düğümün birden çok kimliği bulunmaktadır. Böylece meşru olan A düğümüne kendini meşru bir düğüm olarak gösterebilmektedir. Saldırının gerçekleştirilmesi de gerçekleştirildikten sonra tespit edilmesi de oldukça zordur. Hafif kimlik doğrulama yaklaşımları ve makine öğrenmesi tabanlı davranış izleme yaklaşımları geliştirilerek tespit edilmeye ve önlenmeye çalışılmaktadır.



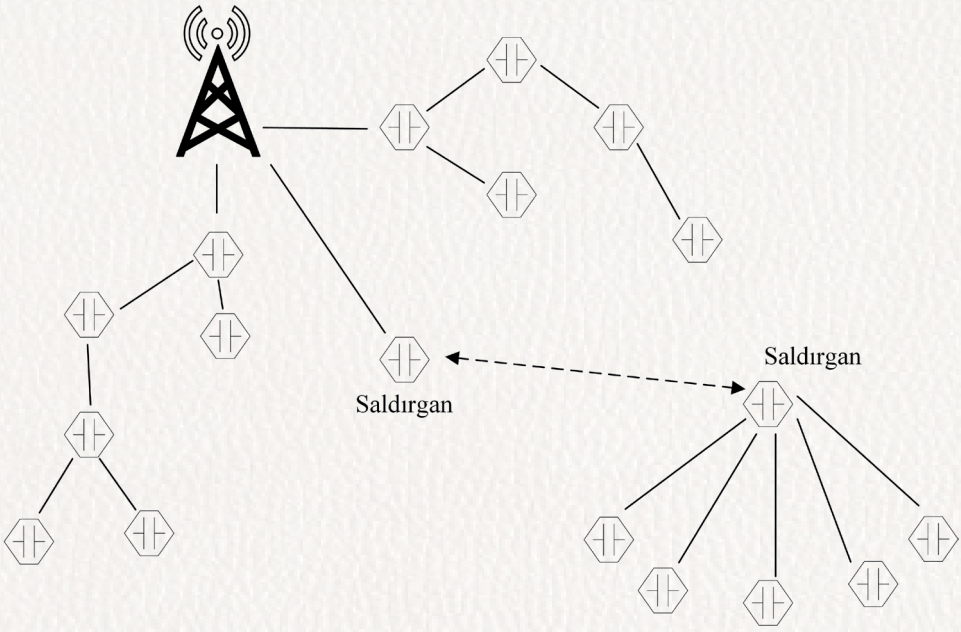
Şekil 1.5. Sybil saldırısı

1.3.2. Wormhole Saldırısı

Ağın bir bölümüne sızan saldırgan, düşük gecikmeli bağlantı üzerinden iletiler alarak bunları bir tünel yoluyla farklı bölümlerde tekrarlayabilir. Wormhole saldırısı, paketleri, tekrarlama yolu ile birbirine olan uzaklıklarını en aza indirgemek isteyen iki düğümden oluşmaktadır [16].

Bir saldırgan iki düğüm arasında yer almakta ve aralarında mesajlar iletilmektedir. Uzaktaki iki düğümü düşük gecikmeli bağlantı sayesinde komşu olduklarına ikna etmektedir. Wormhole sayesinde farklı başka saldırılar da etkinleştirilebilmektedir. Temel olarak, ağın bir bölümünde düşük gecikme süresi üzerinden alınan paketleri tünelleyerek ağın farklı bir bölümünde tekrar oynatmaktadır. Genellikle bu iki bölgelerden biri hedefe yakın diğeri ise baz istasyonuna yakın yerlere konuşlanmaktadır. Wormhole saldırısı Şekil 1.6'da gösterilmektedir. Şekilde iki saldırgan arasındaki kesikli bağlantı gecikmenin düşük olduğunu ifade etmektedir. Her düğümden geçişte zaman damgası gibi bilgiler eklenerek kısa yollar tespit edilmeye çalışılsa da düğüm kesin

bir şekilde saldırgan olarak işaretlenememektedir. Aksi takdirde normalde gecikmesi düşük ve meşru olan bir düğümün çalışması bozulabilmektedir. Bu nedenle saldırının gerçekleştirilmesi de tespit edilmesi de zordur. Bunun için dijital imza, iletim zamanlaması, yönlü anten, istatistiksel analiz ve topolojik bilgiye dayalı yöntemler geliştirilmektedir.



Şekil 1.6. Wormhole saldırı

1.3.3. Fiziksel Saldırılar

IoT sistemler içinde çok sayıda sensörden alınan veriler merkeze gönderilerek sonuçlar alınmaktadır. Belli bir coğrafi bölgeye yayılmış sensörlerin olduğu ortamda düğüm çalınması gibi fiziksel saldırılar da olabilmektedir. Ayrıca sis bilgi işlem kullanan bir IoT uygulamasında depolama ve veri işleme yerel ağda yapıldığı için veri merkezinin konumu uç düğümlere yakındır ve bulunabilmektedir. Sis yapısının bu dezavantajı veri merkezine yapılabilecek olan fiziksel saldırıları kolaylaştırmaktadır. Bu saldırıları önlemek için sunucu odalarının fiziksel olarak da güvenlik önemlerini almak oldukça önemlidir.

1.3.4. Dağıtık Hizmet Reddi (Distributed Denial of Service - DDoS)

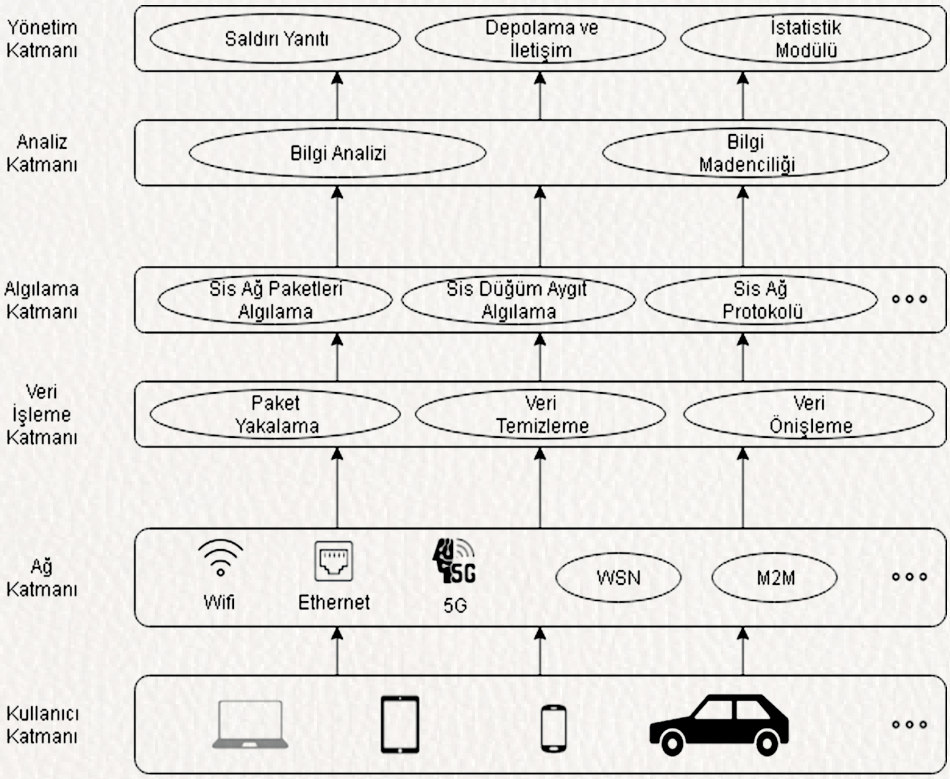
Çoğu bilişim uygulamalarında olduğu gibi sis kullanan IoT sistemlerde de en önemli tehlikelerden biri hizmet reddi saldırılarıdır. Hizmet reddi saldırılarını seçilen kurban bilgisayarlar üzerinden dağıtık bir şekilde yapılması bu saldırıyı çok daha güçlü hâle getirmektedir. Sis bilişim yapılarında DDoS önlemeye yönelik çeşitli çalışmalar yapılmaktadır.

Bulut sunucularını DDoS saldırılarından korumak için ara katman olarak görev yapan sis katmanında belirlenen kurallar ile saldırı tespit edilerek bulutun kaynaklarının boşa kullanımı önlenebilmektedir [17]. Bu işlem sis katmanında, trafiğin saldırı süresine, paketlerin oranına, paket büyüklüğüne ve kullanılan protokole göre filtrelemeler yapılarak gerçekleştirilmektedir.

Sadece bulut sunucularında değil sis sunucularında da DDoS saldırıları yapılmaktadır. DDoS saldırılarını aktifleştirmek için saldırgan öncelikle sisteme Truva atları ve virüsler yerleştirerek kullanıcı tarafındaki cihazları kontrol etmektedir. Saldırılar kullanıcı katmanından gerçekleştirilmektedir. Saldırgan sis kaynakları üzerinde DDoS saldırısı uyguladığında bazı sonuçlar ortaya çıkmaktadır [18]. Bunlar; sis düğümün ağ portunun engellenmesiyle gerçek kullanıcıların ve gerçek verilerin erişim yollarının engellenmesi, sis düğümüne çok sayıda kötü niyetli istek gönderilerek erişim yolunun engellenmesi, sis düğümü ile bulut arasındaki iletişimin engellenmesidir. Sis katmanındaki DDoS saldırısının önlenmesine yönelik olarak geliştirilen sistemlerde, saldırıların tespit edilmesi ve veritabanında kayıt günlüğü tutulması, bulut sunucuları tarafından sis düğümlerinin gerçek zamanlı olarak izlenmesi ve veri madenciliği yöntemleriyle saldırganının davranışına uygun cevabın üretilmesi işlemleri gerçekleşmektedir. Sis düğümlerine DDoS yapıldığı durumda hipergraf teorisine dayalı yöntem ile ağ bant genişliği kaynakları modellenmekte ve Apriori algoritması ile korelasyon analizi yapılmaktadır. Sis ağındaki DDoS saldırısını engelleme modeli Şekil 1.7'de gösterilmektedir [18].

Hipergraf teorisi ve Apriori algoritması tabanlı çözümde simülasyon sonuçlarına göre sis düğümlerindeki kaynak kullanımının daha iyi performansa sahip olduğu gösterilmektedir. Ancak bu alanda yapılan çalışmalar

da sınırlı kalmaktadır. Bu nedenle sis bilişim için daha kapsamlı ve daha iyi sonuçlar üreten DDoS korunma yöntemleri geliştirilmeye çalışılmaktadır.



Şekil 1.7. Sis ağında DDoS saldırı önleme yöntemi mimarisi

Geleneksel bilgisayar ağlarına ve kaynaklarına yapılan saldırıların büyük bir kısmı sis bilişim ağı ve kaynakları için de uygulanabilmektedir. Kablosuz bir ortam ve yerel ağda hizmet verdiği için doğası gereği birçok saldırıya açıktır. Ancak sis tabanlı IoT uygulamaları için saldırı tespit sistemleri, hafif kimlik doğrulama, veri gizliliği ve bütünlüğü yaklaşımları, ağ tıkanıklığını ve veri taşmalarını önleme çerçeveleri, güvenli kablosuz iletim ve rota yanlışlarını önleme çözümleri, etkili kaynak yönetim şemaları gibi çok fazla konuda incelemeler ve geliştirmeler devam etmektedir.

1.4. IOT UYGULAMALARINDA SİS BİLİŞİM KULLANIMINDA GÜVENLİK İHTİYAÇLARI

Sis bilişimin yapısı gereği IoT sistemlerine getirdiği bir takım güvenlik yetenekleri ve olası tehditlere karşı yapılması gereken güvenlik ve gizlilik ihtiyaçları bulunmaktadır. IoT uygulamaları hastane, fabrika, şehir, askeriye, tarım, deniz altı, yer altı, spor gibi çok çeşitli alanlarda kullanılabilmektedir. Hastanede, hastaları izleyen sensörlerden sağlık personelinin cihazlarına veri aktarımı; fabrikada, üretimde kullanılan makinelerin birbirleriyle haberleşmek için veri taşıması; trafikte, akıllı şehir kurulmasında trafik lambalarının birbirleriyle haberleşmesi için verilerin taşınması, askeriyede, sınırlara yerleştirilen sensörler ile ülke giriş-çıkış kontrolünde veri merkezine verilerin taşınması; tarım alanlarında, bitkileri izleyen sensörler ile sulama ihtiyaçlarına yönelik çiftçilere verilerin taşınması, oyun alanındaki sporcuları izleyen sensörlerden teknik ekibe veya kulüp doktorlarına verilerin taşınması gibi işlemler yürütülmektedir. Bunlar dışında daha birçok alanda IoT uygulamaları kullanılmaktadır. Üretilen verilerin cihazlar arasında aktarılırken korunması gerekmektedir. Çünkü kullanılan alana da bağlı olarak verilerin korunmaması hayat kaybı, itibar kaybı, maddi kayıp gibi tehlikeli sonuçlara yol açabilmektedir.

IoT uygulamalarında hesaplama kaynağı olarak genellikle bulut bilişim sistemleri kullanılmaktadır. Bulut sunucuları ile haberleşmede veriler güvensiz olan internet ağı üzerinden geçmek zorundadır. Sis bilişim kullanılan bir uygulamada algılanan veriler güvenlik işlemlerinden (şifreleme, zaman damgası vb.) geçirilerek buluta taşınmaktadır. Sis düğümlerinde kullanılmayan veriler veya buluta gönderilen veriler şifrelenmektedir. Sonuç olarak, sis bilişim IoT uygulamalarına doğrudan bir güvenlik mekanizması sağlayabilmektedir.

Sis bilişim gecikmeyi azaltmak için bulut ve kullanıcı arasında önemli bir ara katmandır. Sis bilişimde gecikmesinin düşük olması gerçek zamanlı ve gerçek yaşam IoT uygulamalarının kullanılabilmesini sağlamaktadır. Sis düğümleri çok büyük verileri bulut kararlılığında işleyebilmektedir. Ancak düşük gecikmenin yanı sıra ek bir ara katman olması gizliliğe ve hesap verebilirliğe karşı yapılan güvenlik tehditlerini arttırmaktadır. IoT uygulamaları için sis

bilişimdeki güvenlik ve gizlilik gereksinimleri ile başlıca zorluklar şu şekilde listelenebilir [11] [19]:

- **Kimlik Doğrulama:** Kaynak kısıtlı IoT cihazları kimlik doğrulama için gereken şifreleme işlemlerini gerçekleştirememektedir. Bunun için yüksek maliyetli olan depolama ve veri işleme ihtiyaçlarını sis düğümleri gibi dış kaynaktan sağlamaktadır. Bu tür sistemlerde Ortak Anahtar Altyapısı (PKI) kullanan geleneksel kimlik doğrulama sistemleri uygun değildir. Bu yüzden güvenli iletişim için çok noktaya yayın kimlik doğrulamasına dayanan sistemler geliştirilmektedir. Akıllı şebeke için geliştirilen geniş alanlı ölçüm sistemi anahtar yönetimi bunlardan biridir [20]. Kullanıcılar kesintisiz hizmet almak için sis ağında kimliklerini doğrulamaktadır. Yetkisiz kullanıcıların erişimi engellenmektedir. Ayrıca kötü niyetli düğümler kimlik doğrulama gereksinimi ile belli ölçüde kısıtlanmaktadır.
- **Veri Koruma:** IoT uygulamalarında cihaz sayısına bağlı olarak büyük miktarda veri üretilebilmektedir. Bu verilerin işlenmesi ve depolanması sis düğümlerinde yapılmaktadır. Kaynak kısıtlı IoT cihazları tarafından verilerin doğruluğunu belirlemek maliyetli olduğu için sis düğümleri tarafından veri bütünlüğünün ve gizliliğinin sağlaması gerekmektedir.
- **Gizlilik:** IoT uygulamaları genellikle konum tabanlı servislerdir. IoT cihazları tarafından üretilen verilerin ve cihazların konum bilgilerinin gizli olması gerekmektedir. Kaynak kısıtlı IoT cihazları verileri şifreleme veya şifre çözme yeteneğine sahip değildir. Bu veri işleme durumları sis düğümleri tarafından gerçekleştirildikten sonra veriler buluta gönderilmektedir. Ancak verinin IoT düğümünden sis düğümüne gönderilmesi esnasında gizliliğinin sağlanması gerekmektedir. Bir başka deyişle, IoT cihazları bilgi işleme ve depolama gereksinimlerini sis düğümüne yükleyebilir fakat güvenlik gereksinimlerini yükleyemez. IoT cihazları sadece bilgi işleme ve depolama durumunda sis ile iletişime geçmektedir. Bunun haricinde hiçbir iletişim durumu sis ağının bir parçası değildir. Güvenli iletişim için IoT cihazı bilgi işleme ve depolama gereksinimi olduğunda sis ağındaki –varlığından

bile haberdar olmadığı– herhangi bir sis düğümü ile iletişime geçmektedir. Bu iletişimi güvence altına almak için anahtarların önceden paylaşılmasını gerektiren simetrik şifreleme yapıları uygun değildir. Asimetrik şifreleme yapıları ise maliyeti yüksek olduğundan kaynak kısıtlı IoT cihazları için uygun değildir. Sis düğümlerine gelen verilerin gizlenmesi ve güvenli iletişimin sağlanması konusunda yöntemler sınırlıdır.

- **Doğruluk:** IoT uygulamaları güvensiz bir ortamda çalışmaktadır. Bu ortamlarda kullanılan servislerin doğruluk açısından güvenli olduğuna karar verme işi genel güvenliği oluşturan parçalardır. Sistemlerin doğru çalıştığından emin olmak için servislerin güvenilirliğini koruma, hatalı davranış sorunlarını giderme, kötü niyetli davranış tespiti gibi modeller geliştirilmektedir [19]. Bu modeller genellikle cihazlar arasında iki yönlü güven mekanizmasının sağlanması temeline dayanmaktadır. Sis için iki taraflı doğrulamayı sağlamak zordur.
- **Erişim Kontrolü:** Yalnızca meşru kullanıcıların IoT cihazlarına erişimini sağlayan, diğer düğümleri sınırlandıran güvenlik mekanizmalarıdır. IoT cihazları kaynak kısıtlı olduğu için erişim kontrolünü sağlamak zordur. Bu yüzden cihazların doğrulanması için Sertifika Yetkilisi (CA) olarak görev yapan üçüncü taraf gerekmektedir.
- **Kötü Amaçlı Saldırı ve Yetkisiz Giriş Tespiti:** IoT ortamında bulunan kötü niyetli bir düğüm verilerin hatalı iletilmesine, değiştirilmesine veya üzerinden geçen verilerin çalınmasına yol açmaktadır. Yüzlerce düğümden oluşan IoT ağında cihazlar kaynak kısıtlı olduğu için sis düğümleri ile birbirlerini doğrulayamamaktadır. Ağdaki cihazların çoğu karşılıklı olarak birbirini doğrulayamadığından saldırgan düğüm sis düğüme sürekli olarak depolama veya veri işleme isteği göndererek DoS (Denial of Service - Hizmet Reddi) atağı başlatabilmektedir. Kötü niyetli düğümden korunmak için Wi-Fi tabanlı ağlarda düğümlerin erişimi sınırlandırılmaktadır. Şifreleme ve erişim kontrolü gibi güvenlik yaklaşımları buluttaki verileri korumaya çalışmaktadır. Ancak yanlış yapılandırılmış servisler, hatalı uygulama gibi nedenler bu

yaklaşımları karmaşık saldırılara karşı güvensiz hâle getirmektedir. Saldırgan ağa sızdıktan sonra, kullanıcı davranışı izlenerek olası anormal durumlar tespit edilebilmektedir. Anormallik tespit edildiğinde belirli güvenlik adımlarından geçirilerek düğümün doğrulandığı yapılar geliştirilmektedir [21].

- **Veri Bütünlüğü:** Sis düğümlerinde meydana gelebilen ortadaki adam gibi saldırılarda oluşan verilerin bozulması durumlarının sis tarafından algılanması gerekmektedir. Veri bütünlüğünü bozarak kullanıcıya hatalı verilerin gitmesine sebep olan bu tür durumlar sis tarafından düzeltilmelidir.
- **Kullanılabilirlik:** Sis düğümlerinin, kullanıcıların sistem kaynaklarından her an hizmet almasını engellemeye yönelik yapılan saldırılardan korunması gerekmektedir. Hizmet Reddi (DoS) ve Dağıtık Hizmet Reddi (DDoS) kullanılabilirliği etkileyen saldırılardan bazılarıdır.
- **Heterojenlik:** Farklı özellikteki çok sayıda cihazdan verilerin sis merkezine iletilmesi gerekmektedir. Farklı iletişim ihtiyaçları karşılandığında hesaplama gücü ve maliyet artmaktadır.
- **Hesaplama Maliyeti:** Mimaride, gecikmeyi azaltmak için eklenen sis ara katmanının veri işlemek, depolamak, gerçek zamanlı yanıt oluşturmak, saldırıları tespit etmek vs. için hesaplama gücüne ihtiyacı vardır. Ancak hesaplama maliyetinin optimize edilmesi gerekmektedir.
- **Anahtar Yönetimi:** Cihazlar kimlik doğrulama aşamasında oturum anahtarları oluşturulmaktadır. Bu anahtar çiftinin yönetimi oturumun güvenliği için oldukça önemlidir.
- **Güvenilir Taraf:** İletişimde yer alan her cihazın bilgileri korunmalı ve güncellenmelidir. Bunun için önyükleme yapan, anahtarları yöneten ve tüm IoT cihazlarına anahtar atayan güvenilir bir üçüncü taraf yöntemi ve bulutu tamamen güvenilir hâle getirmek veya her bir sis düğümünde kimlik doğrulama yapan yöntemdir. Güvenilir olanı seçmek önemlidir.

IoT uygulamaları için sis bilişimde karşılaşılan saldırı çeşitleri ve sis ortamının hangi alanında faaliyet gösterdiği Tablo 1.3'te gösterilmektedir [14].

Tablo 1.3. Sis bilişim saldırı çeşitleri ve etki alanı

Etki Alanı	Saldırılar
Ağ Altyapısı	Hizmet Reddi (DoS), Aradaki Kişi (Man In The Middle), Sahte Geçit Yolu (Rogue Gateway)
Bulut Veri Merkezi	Hizmet Reddi, Gizlilik Zafiyeti, Kimlik Doğrulama Saldırıları, Yetki Yükseltme (Privilege Escalation), Hizmet Manipülasyonu, Sahte Veri Merkezi
Sis Veri Merkezi	Fiziksel Zarar, Gizlilik Zafiyeti, Kimlik Doğrulama Saldırıları, Kötücül Yazılım Enjeksiyonu (Malware Injection), Yetki Yükseltme, Hizmet Manipülasyonu, Sahte Veri Merkezi
Sanallaştırma Altyapısı	Hizmet Reddi, Kaynakların Kötüye Kullanımı, Gizlilik Zafiyeti, Yetki Yükseltme, Sanal Makine Manipülasyonu
Uç Cihazlar	Fiziksel Zarar, Kimlik Doğrulama Saldırıları, Kötücül Yazılım Enjeksiyonu, Bilgi Enjeksiyonu, Hizmet Manipülasyonu

1.5. IOT UYGULAMALARINDA SİS BİLİŞİM KULLANIMI

Bu bölümde IoT uygulama geliştirme aşamalarında sis bilişimin dâhil edilmesi için kullanılan araçlar ve ortamlar anlatılmaktadır. IoT uygulamalarına akıllı taşımacılık sistemleri, akıllı sağlık hizmetleri, kamu güvenliği, akıllı şebeke, endüstri 4.0, akıllı evler ve akıllı binalar örnek gösterilebilir. Bu uygulamalarda oluşan yüksek miktardaki verilerin işlenmesi ve depolanması için sis bilişim ile bulut bilişim birlikte kullanılabilmektedir. Sis mimari geliştiricilerinin ortak amacı, açık ve kapsamlı bir referans mimarisi oluşturmak, sis bilişimin IoT uygulama alanlarında kullanılmasını sağlamak ve standardını geliştirmektir. Bu kapsamda, sis bilişimi IoT uygulamalarına dâhil etmek için sis bilgi işlem platformları geliştirilmiştir. Bu platformlar şu şekilde listelenebilir [22]:

- **Yazılım Platformları:** IoT uygulamalarının sis altyapısı yerleştirilmesi ve yürütülmesi için gerekli temel işlevleri sağlayan ortamdır. Ticari platformlar ve açık kaynak platformlar olarak ikiye ayrılmaktadır. Ticari platformlar; Nebbiolo, FogHorn Lightning, Cisco IOx, Dell Edge Device Manager, IBM Watson IoT. Açık kaynak platformlar; Microsoft Azure IoT Edge, FogFlow, OpenStack++.

- **Geliştirme Çerçeveleri:** IoT için sis uygulamalarının geliştirilmesini kolaylaştıran ve geliştiricinin detaylara değil uygulamanın mantığına odaklanmasını sağlayan araçlardır. Bu araçlar kütüphaneler, mikro sistemler, soyutlama katmanları, arayüzler, belli başlı kontroller gibi yapılardır. Yazılım platformlarıyla bağlantılı olarak ticari platformlar ve açık kaynak platformlar olarak ikiye ayrılmaktadır. Ticari platformlar; Nebbiolo SDK, FogHorn Lightning SDK, Cisco IOx SDK. Açık kaynak platformlar: EdgeXFoundry (Linux, Java), macchina.io.
- **Donanım Platformları:** Donanım platformları, önde gelen donanım üreticileri tarafından sağlanan sis düğümü rolü üstlenebilen cihazları kapsamaktadır [22]. Şifreleme anahtarlarının korunması ve donanımsal zafiyeti önlemek için IBM tarafından geliştirilmekte olan Kuantuma Dayanıklı Güvenilir Platform Modülü (A Quantum-Resistant Trusted Platform Module - QR-TPM) kullanılmaktadır [23]. IoT uygulamaları için de QR-TPM önemli bir bileşendir. Donanım platformu geliştiren donanım üreticileri; IBM, Nebbiolo Tech, TT Tech, Cisco, Intel, Dell, Raspberry Pi Foundation, Qualcomm vs.

Bu platformlar IoT uygulamaları içine sis hesaplama ağını entegre etmek ve IoT uygulaması geliştirmek için kullanılmaktadır. Platform uygulamalarında da güvenli kod ve donanım geliştirilmeye dikkat edilmelidir. Aksi takdirde oluşan zafiyetler üzerinden bazı saldırılar aktifleştirilebilmektedir. Bağlantılı araçlar, kablosuz sensör ağlar, akıllı şebeke vb. IoT uygulamalarında sis bilgi işlem yapısı kullanılabilmektedir.

1.5.1. Bağlantılı Araçlar (Connected Vehicles)

Bağlantılı araçlar için arabadan arabaya, arabadan Wi-Fi, 3G, LTE (Long Term Evolution - Uzun Süreli Gelişim) gibi erişim noktalarına ve erişim noktasından başka bir erişim noktasına olacak şekilde zengin bir senaryo sunmaktadır [1]. Akıllı trafik ışığı gibi uygulamalar bağlantılı araçlara örnek olarak verilebilmektedir. Bu uygulama, yaya veya bisikletli gördüğünde mesafesine göre ışığı koordine etmektedir. Ayrıca diğer trafik ışıklarıyla da bağlantılı olduğu için ambulans, polis gibi araçların acil durumlarında yeşil

dalgası oluşturmaktadır. Bu tarz uygulamalarda gerçek zamanlı işlemler gerçekleştiği için gecikme süresinin az olması oldukça önemlidir. Bu nedenle sis ağı kullanılmaktadır.

1.5.2. Kablosuz Sensör Ağlar (Wireless Sensor Networks - WSN)

Kablosuz Sensör Ağları, pil ömrünü uzatmak ve enerji tasarrufu sağlamak için düşük güçte çalışmak zorundadır. Düşük güce sahip sensör cihazları (nem, sıcaklık, yağış miktarı, ışık yoğunluğu vs.) verileri algılamanın ötesine geçememektedir. Kaynakları oldukça kısıtlı olan bu cihazlar açma, kapatma, hareket etme, odaklanma, hedefleme, hesaplama, depolama gibi işlevlerini gerçekleştirebilmek için sis ağını kullanabilmektedir. Yakınlık, konum bilinci, hiyerarşik yapısı, mobilite desteği gibi destekleri ile sis bilişim sistemleri WSN uygulamaları için etkili bir yaklaşımdır.

1.5.3. Akıllı Şebeke (Smart Grid)

Akıllı şebeke sistemleri, elektrik şebekelerini akıllı sayaçlar, akıllı üretim araçları, akıllı istasyonlar gibi yöntemler ile izleyen ve kontrol eden yapılardır. Mevcut elektrik enerjisi sistemini rüzgâr gibi yenilenebilir enerji kaynaklarını da içerecek şekilde genişletmektedir [24]. Gerçek zamanlı işlem gerektirdiği için akıllı şebeke uygulamasında sis ağı kullanımı uygundur. Şebeke sensörleri ve cihazları tarafından elde edilen veriler sis ağına iletilmektedir. Makineden Makineye (Machine to Machine – M2M) iletişim için tasarlanan bu sis tabanlı yöntem verileri işledikten sonra kontrolünü de yapmaktadır. Daha sonra veriyi görselleştirme ve raporlama işlemleri yapılan yüksek seviyeye, insan-makine etkileşimine göndermektedir. Seviye ne kadar fazla ise coğrafi kapsam da o ölçüde geniş demektir. Geniş coğrafi alana yayılan sistemlerde sis bilişim verimli çalışmaktadır.

Bu alanlarda sis bilişim sistemleri hâlihazırda kullanılmaktadır. Bunların dışında gerçek zamanlı, düşük gecikme, yüksek işlem gücü, enerji tasarrufu, güvenlik gerektiren ve veri merkezine yakın konumda ve hareketli olan uç cihaz barındıran IoT uygulamalarında da sis bilişim sistemlerinin kullanılması uygundur.

1.6. SONUÇ VE DEĞERLENDİRMELER

Gerçek zamanlı uygulamalarda gecikme süresinin az olması, mobilite desteği, konum farkındalığı ve geniş coğrafi alanlara yayılabilmesi nedeni ile sis bilişim kullanılmaktadır. IoT uygulamalarında kaynak kısıtlı uç cihazlardan elde edilen veriler hesaplama ve depolama amacıyla sis düğümlerine gönderilmektedir. Veriler işlendikten sonra hem uç cihazlara geri bildirim yapılabilmekte hem de veriler bulut sunucularına gönderilebilmektedir. Tüm bu işlemler gerçekleşirken veriler güvenli bir şekilde iletilebilmektedir.

Bu bölümde incelendiği, aktarıldığı ve karşılaştırıldığı gibi;

- Bulut, sis ve kenar bilişim sistemleri özellikle güvenlik tehditleri yönünden karşılaştırıldığında birlerine oldukça benzemektedir. Bulut sunucularına internet aracılığıyla erişim olduğundan diğerlerine göre daha fazla tehdit ile karşı karşıya kalmaktadır.
- Sis bilişimin karşılaştığı tehditler ise katmanlar bazında incelendiğinde uç cihazlara genellikle fiziksel saldırılar, ağ alt yapısı, bulut, sis gibi katmanlarına ise genellikle yazılımsal saldırılar yapılmaktadır. Daha güvenli sis mimarileri üretmek ve bu saldırılardan korunmak için çalışmalar yapılmaktadır.
- Sis bilişimin IoT uygulamalarında kullanılması için gerekli olan platformlar değerlendirildiğinde yazılımsal, donanımsal ve geliştirme ortamları olmak üzere üç bileşenden oluşmaktadır. Donanımlar sis mimarisini gerçekleştirmek için kullanılan tüm aygıtlardır. Geliştirme ortamları sis uygulaması geliştirilirken kullanılan araçlardır. Yazılımlar ise geliştirilen uygulamanın çalışmasını sağlayan yapılardır. Bu bileşenlerin güvenli kod ve güvenli donanım mantığıyla geliştirilmesi tüm sistem güvenliği için son derece önemlidir. Ayrıca, birbirlerini destekleyen ürünler kullanılarak sis uygulaması geliştirilmesi sistem performansı açısından önemlidir.
- IoT uygulamalarında amaç ölçeklenebilir, merkezi olmayan, verimli ve güvenli bir altyapının geliştirilmesi olduğu için uygulamalarda sis bilişim yapısının önemli bir yeri vardır. Çünkü sis bilişim verilerin yerelde işlenmesini ve buluta gönderilecek verilerin güvenli bir şekilde yapıl-

masını sağlayabilmektedir. Uç cihazlardan algılanan veriler yerel ağdaki sis sunucularında işlendiği için yanıt süresi bakımından oldukça verimli uygulamalar geliştirilebilmektedir. Ancak böyle bir alt yapıya sahip sis mimarilerinin geliştirilmesi üzerine çalışmalar devam etmektedir.

Sonuç olarak; sis bilişim için çalışılması ve geliştirilmesi gereken en önemli konulardan biri, sisin katmanlarında karşılaştıkları güvenlik tehditlerini algılayan ve önleyen yapıların geliştirilmesi; sis kapsama alanına giren bir düğümün saldırgan olup olmadığını belirlemek için konumunun belirlenmesi; DDoS ataklarına karşı etkili çözümler geliştirilmesi, gizliliğin sağlanması, dağıtılmış ve ölçeklenebilir güvenli sis bilişim alt yapılarının oluşturulması; bu konuda yapılması gereken güvenlik çalışmalarından bazıları olup bu çalışmalara daha çok önem gösterilmelidir. Ayrıca, sis bilişim sistemlerindeki bu zorluklara çözüm kapsamında son yıllarda yapılan çalışmalardaki eğilim yapay zekâ, makine öğrenmesi ve optimizasyon tabanlı güvenlik yaklaşımları geliştirmek yönündedir.

Teşekkür

Bu araştırma, PYO.MUH.1906.17.003 numaralı OMÜ projesi tarafından desteklenmektedir.

KAYNAKLAR

[1] K. K. Patel, S. M. Patel, "Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges", *International journal of engineering science and computing,* 2016, vol. 6, no. 5, pp. 6122-6131.

[2] F. Bonomi, R. Milito, J. Zhu, S. Addepalli, "Fog computing and its role in the Internet of things", *Proc. 1st Edition MCC Workshop Mobile Cloud Comput.*, Helsinki, Finland, 2012, pp. 13-16.

[3] https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf (Erişim Zamanı: 13.06.2019).

[4] S. Yi, C. Li, Q. Li, "A survey of fog computing: Concepts applications and issues", Proc. ACM *Workshop Mobile Big Data*, 2015, pp. 37-42.

[5] F. Y. Okay ve S. Ozdemir, "Routing in Fog-Enabled IoT Platforms: A Survey and an SDN-Based Solution," in *IEEE Internet of Things Journal*, vol. 5, no. 6, 2018, pp. 4871-4889.

[6] C. Mouradian, S. Kianpisheh, M. Abu-Lebdeh, F. Ebrahimnezhad, N. T. Jahromi ve R. H. Glitho, "Application Component Placement in NFV-Based Hybrid Cloud/ Fog Systems With Mobile Fog Nodes," in *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 5, 2019, pp. 1130-1143.

[7] H. Madsen, B. Burtschy, G. Albeanu ve F. Popentiu-Vladicescu, "Reliability in the utility computing era: Towards reliable Fog computing," *2013 20th International Conference on Systems, Signals and Image Processing (IWSSIP)*, Bucharest, 2013, pp. 43-46.

[8] X. Wang, M. Chen, T. Taleb, A. Ksentini ve V. C. M. Leung, "Cache in the air: exploiting content caching and delivery techniques for 5G systems," in *IEEE Communications Magazine*, vol. 52, no. 2, 2014, pp. 131-139.

[9] W. Liu, T. Nishio, R. Shinkuma, T. Takahashi, "Adaptive resource discovery in mobile cloud computing", *ACM Comput. Commun.*, vol. 50, 2014, pp. 119-129.

[10] J. Ni, K. Zhang, X. Lin ve X. S. Shen, "Securing Fog Computing for Internet of Things Applications: Challenges and Solutions," in *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, 2018, pp. 601-628.

[11] M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, N. Choudhury, V. Kumar, "Security and Privacy in Fog Computing: Challenges," in *IEEE Access*, vol. 5, 2017, pp. 19293-19304.

[12] A. Bader, H. Ghazzai, A. Kadri ve M. Alouini, "Front-end intelligence for large-scale application-oriented internet-of-things," in *IEEE Access*, vol. 4, 2016, pp. 3257-3272.

[13] B. Varghese, N. Wang, S. Barbhuiya, P. Kilpatrick ve D. S. Nikolopoulos, "Challenges and Opportunities in Edge Computing," *2016 IEEE International Conference on Smart Cloud (SmartCloud)*, New York, NY, 2016, pp. 20-26.

[14] R. Roman, J. Lopez, M. Mambo, "Mobile edge computing Fog et al.: A survey and analysis of security threats and challenges", *Future Generation Computer Systems*, vol. 78, 2018, pp. 680-698.

[15] S. R. Rajeswari, V. Seenivasagam, "Comparative Study on Various Authentication Protocols in Wireless Sensor Networks," *The Scientific World Journal*, 2016, pp. 1-16.

[16] C. Karlof, D. Wagner. UC Berkeley. https://cs.gmu.edu/~setia/cs818/lectures/secure-routing.pdf (Erişim Zamanı: 31.07.2019).

[17] Deepali, K. Bhushan, "DDoS Attack Defense Framework for Cloud using Fog Computing," *2.IEEE International Conference on Recent Trends in Electronics Information & Communicstion Technology, RTEICT*, 2017, pp. 534-538.

[18] X. An, J. Su, X. Lü, F. Lin, "Hypergraph clustering model-based association analysis of DDoS attacks in fog computing intrusion detection system," *EURASIP Journal on Wireless Communications and Networking*, 2018, pp. 1-9.

[19] A. Alrawais, A. Alhothaily, C. Hu ve X. Cheng, "Fog Computing for the Internet of Things: Security and Privacy Issues," in *IEEE Internet Computing*, vol. 21, no. 2, 2017, pp. 34-42.

[20] Y. W. Law, M. Palaniswami, G. Kounga ve A. Lo, "WAKE: Key management scheme for wide-area measurement systems in smart grid," in *IEEE Communications Magazine*, vol. 51, no. 1, 2013, pp. 34-41.

[21] S. J. Stolfo, M. B. Salem ve A. D. Keromytis, "Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud," *2012 IEEE Symposium on Security and Privacy Workshops*, San Francisco, CA, 2012, pp. 125-128.

[22] C. Puliafito, E. Mingozzi, F. Longo, A. Puliafito, O. Rana, "Fog Computing for the Internet of Things: A Survey," *ACM Trans. Internet Technol.*, Article 18, April 2019.

[23] https://futuretpm.eu/downloads/deliverables/FutureTPM-D2.1-First-Report-New-QR-Cryptographic_PU_M09.pdf (Erişim Zamanı: 29.05.2019).

[24] A. Bari, J. Jiang, W. Saad, A. Jaekel, "Challenges in the smart grid applications: An overview," *International Journal Distributed Sensor Networks*, vol. 2014, 2014, pp. 1-12.

Bölüm 2

SALDIRI TESPİT SİSTEMLERİ VE LOG (GÜNLÜK) ANALİZİ

Hidayet Takcı

Bilişim sistemlerine her geçen gün farklı türlerde ve farklı yoğunluklarda saldırılar meydana gelmektedir. Yapılan saldırıların ve yetkisiz erişimlerin takibi ve analizi ileride yapılacak saldırıları engelleme için bir ihtiyaçtır. Bu ihtiyaca karşılık olarak bilişim sistemlerine yapılan saldırıları tespit ve izleme görevi gören ve saldırı tespit sistemi adını alan yazılım ve donanımlar geliştirilmiştir. Bu çalışmanın amacı saldırı tespit sisteminin fonksiyonlarını ortaya koyduktan sonra türleri ve örnekleri hakkında bilgi vererek konuyu aydınlatmaktır. Ayrıca bu alanda daha önce yapılmış bir uygulama yardımıyla bir saldırı tespit sisteminin nasıl geliştirilebileceğine dair bilgi verilmiştir. Örnek uygulama saldırı tespitinde veri madenciliği tekniklerini kullanmaktadır.

2.1. GİRİŞ

Son dönemde bilişim teknolojilerinde şahit olduğumuz gelişmeler birçok işin bilgisayar sistemlerine dayalı olarak yapılmasına imkân tanımıştır. Bilişim sistemlerinin gelişiminden; eğitim, sağlık, finans, bankacılık, askerî sistemler ve devlet başta olmak üzere hemen her sektör olumlu yönde etkilenmiştir. Son dönemde artan bir ilgiyle geliştirmeleri devam eden yapay zekâ çalışmaları dâhil olmak üzere hemen her şey bilişim teknolojilerinin gelişimiyle paralel gelişmiştir.

Bir taraftan bilişim sistemlerinde baş döndürücü gelişmeler yaşanırken diğer taraftan bilişim sistemlerine yapılan saldırılarda artış gözlenmektedir. Devlete ait sistemler, sağlık sistemleri, bankacılık ve askerî sistemler yasal kullanıcıların hizmet aldığı sistemler olmakla birlikte bilgisayar korsanlarının da bir numaralı hedefidir. Dolayısıyla bu ihtiyaçlar nedeniyle bilişim güvenliği konusunu gündeme girmiştir.

Bilişim güvenliği konusu ilk olarak "Morris kurdu" adı verilen bir zararlı yazılım ile dikkatleri üzerine çekmeyi başarmıştır [1]. Morris kurdu başarılı şekilde bilişim sistemlerine yayılmış ve bilgisayar sistemlerini çalışamaz hâle getirmiştir. Güvenlik önlemleri olarak başta güvenlik duvarı (GD) olmak üzere çeşitli yazılıma ve donanıma dayalı çalışmalar yapılmıştır. Bilişim güvenliği konusundaki son durum eskisinden daha karmaşık bir hâl almıştır. Her gün yeni bir zararlı yazılım piyasaya çıkmakta ve önemli derecede zarara neden olabilmektedir. Güvenlik etki alanındaki çalışmalar yavaş bir tempoda devam ederken kötü amaçlı yazılımlar daha hızla ortaya çıkmakta ve ihlallerde yeni boyutlara ulaşmaktadırlar.

Bilişim sistemlerini güvenli hâle getirmenin ilk adımı konuyu mühendislik disiplini içerisinde ele almak ve güvenliği ilgilendiren her konuyu denkleme katmak olacaktır. Bu kapsamda bilgi güvenliğinin kabaca teknik paydaşları; bilgisayar sistemleri, işletim sistemi, ağ ortamı, web sunucusu ve diğer sunucular, güvenlik duvarları, saldırı tespit ve engelleme sistemleri, virüs ve diğer zararlı yazılımlar ile güvenlik politikasıdır.

Bu çalışmada bilişim güvenliğinin paydaşlarından birisi olan saldırı tespit sistemleri ele alınacaktır. Saldırı tespit sistemleri genellikle güvenlik duvarlarının gerisinde kalmaktadır. Bu durumun en önemli sebebi saldırı tespit sistemlerinin güvenlik duvarlarına yardımcı bir görev üstlenmesidir. Güvenlik duvarlarının paket filtreleme kuralları ve vekil (proxy) erişim kontrolü uygulamaları karmaşıktır ve genellikle hata yapılmaktadır. Yapılan hatalar nedeniyle sızmalar meydana gelmekte ve maalesef saldırganlar güvenlik duvarını atlatarak iç ağa girebilmektedir. Güvenlik duvarından geçen saldırganların ve içeride bulunan saldırganların yakalanması için saldırı tespit sistemleri bir ihtiyaçtır. Ek olarak saldırı tespitinin yapılmasını gerekli hâle getiren bazı hâller bulunmaktadır:

- Kerberos gibi önemli güvenlik çözümü üreten firmaların dahi ürünleri kırılabilmiştir. Dolayısı ile en iyi şifreleme teknolojisi dahi güvenlik için yeterli olamamaktadır. Ek tedbirlere ihtiyaç vardır.
- Zayıf formlu işleme programları sayesinde web sunucuya zararlı veriler girilebilmektedir. Bunun bir neticesi olarak saldırganlar hedef sisteme sızabilmekte ve yerleşebilmektedirler.
- Özel anahtarlar çözülmüş formda saklanabilirler fakat kullanıcı seçimli bir parola bu anahtarlara erişim için zayıflığa sebep olabilir. Çalışanlar, ziyaretçiler ve diğerleri zararlı program veya kodlar gönderebilirler. Bu durumda da ağ içerisinden yapılacak saldırıların tespit edilmesi ihtiyacı saldırı tespit sistemlerini mecburi hâle getirmektedir.
- Mevcut sistemlerin birçoğunda saldırıya ve sızmaya imkân verecek zafiyetler bulunmaktadır. Bu zafiyetlerin tamamının ortadan kaldırılabilmesi teknik ve ekonomik nedenlerden dolayı mümkün değildir.
- Zafiyetleri bilinen sistemlerin daha güvenli sistemlerle yer değiştirmesi çoğu zaman mümkün olamamaktadır. Çünkü güvenli olmayan sistemde bulunan bütün özellikler güvenli olan sistemde bulunmayabilir veya değiştirilmesi çok fazla maddi yük getirebilir.
- Tam güvenliğe sahip sistemlerin geliştirilmesi ya çok zordur ya da imkânsızdır. En güvenli sistem bile yetkisini kötüye kullanan kişiler için herhangi bir şey yapamamaktadır [2].

Güvenlik uzmanları; bilişim sistemlerini yetkisiz erişimlerden korumaya ve sistemlerin kesintiye uğramadan çalışmasına gayret gösterirler. Bu işlemleri güvenlik politikası adı verilen rehber çerçevesinde yerine getirirler. Güvenlik politikası bir bilişim sistemini ihlallerden korumak için geliştirilmiş ve kurumda bulunan herkes tarafından uyulması gerekli politikaları vermektedir. Güvenlik politikaları; hassas verinin bilişim sistemlerinde saklanması, aktarımı, dağıtımı ve yönetimi ile ilgili ilke ve kuralların tamamını içerir.

Güvenlik politikasını uygulamada yardımcı seçeneklerden birisi saldırı tespit sistemleridir. Saldırı tespit sistemleri bilişim sistemlerindeki hareketleri

izleyen ve analiz eden yazılım ve donanımlardır. Saldırı tespiti sistemlerinin izleme görevi için ona denetim (audit) mekanizması yardım eder. Denetim mekanizması tarafından kayıt altına alınan aksiyonlar saldırı tespit sistemleri tarafından analiz edilerek işlem yerine getirilir. İşletim sistemlerinde ve dolayısı ile saldırı tespiti ile aslında güvenlik politikasındaki tanımlara göre saldırı olarak kabul edilen durumların tespiti yerine getirilir.

Bilişim sistemlerine saldırı sırasında kullanıcıların sıklıkla kullandığı yöntemler aşağıda verilmiştir.

- Servis reddi (DoS)
- Tarama ve bulma
- Şifre saldırıları
- Başka kullanıcıların hakkına sahip olma
- Truva atı
- Karşı sistemi tahrip
- Suistimal
- Log dosyalarının silinmesi
- Güvenlik mimarisinin değiştirilmesi

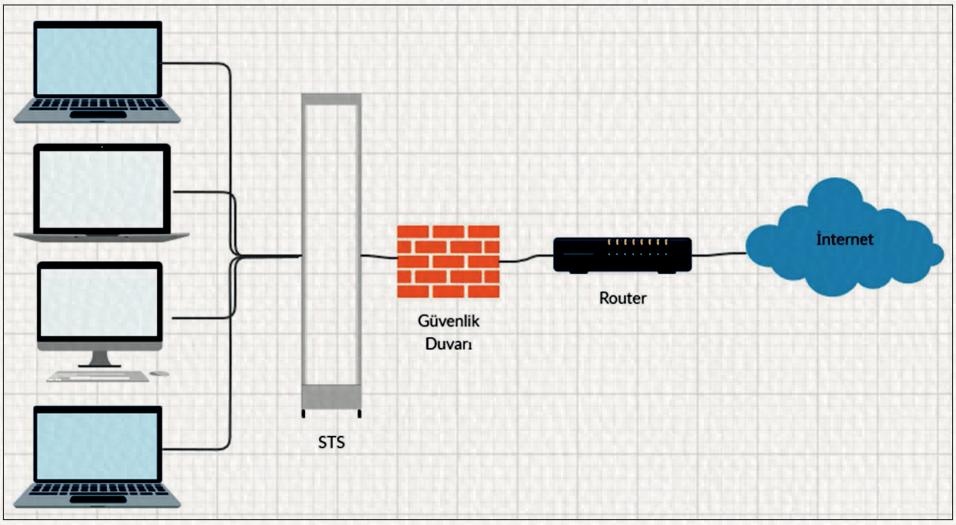
Bu saldırı yöntemlerinin hepsi için de örüntülerin tanımlanması ve analizi mümkün olacaktır. Örneğin, servis reddi için sıklıklara dayalı, suistimal tespiti için kurallara dayalı yöntemler kullanılabilmektedir.

Güvenlik politikasının yaptırımı önemli bir konudur başka önemli bir konu ise ihlallerin tespit edilmesidir. İhlallerin tespitinde bilişim sistemlerini izleme görevi yapan uygulamalar kullanılır. Saldırı tespit işlemi, bilişim sistemlerinin yetkisi olmayan kişi veya uygulamalar tarafından kullanımını tespit etme çalışmasıdır [3].

Saldırı tespiti için başta yukarıda verilen saldırı türleri olmak üzere imza tabanlı ve anormallik tabanlı teknikler kullanılmaktadır. Bu teknikleri destekleyen önemli disiplinlerden birisi veri madenciliğidir. Büyük miktardaki veriden anlamlı bilgiyi bulmaya yarayan veri madenciliği tek başına bir saldırı tespit tekniği değil saldırı tespit işlemleri için faydalı modeller sunan yöntemler bütünüdür.

2.2. SALDIRI TESPİT SİSTEMLERİ

Saldırı tespit sistemleri sistem veya ağ kaynakları üzerinde meydana gelen nüfuz girişimleri veya anormallikleri gözlemleyerek onlar hakkında veri toplayan ve daha sonra toplanan verileri analiz ederek şüpheli durumları sistem yöneticisine alarmlar yoluyla bildiren yazılım veya donanımlardır [4]. Bu sistemler tek bir bilgisayarın korunmasından büyük bir ağın korunmasına kadar büyük bir yelpazede hizmet verir [5]. En temel sınıflandırma ağ tabanlı saldırı tespit sistemleri (NIDS) ve konak tabanlı saldırı tespit sistemleri şeklindedir (HIDS). Basit bir ayrım olarak işletim sistemi günlüklerini analiz eden sistemler konak tabanlı sistemler, ağ üzerindeki trafiği analiz eden sistemler ise ağ tabanlı saldırı tespit sistemleri olarak bilinir.



Şekil 2.1. Saldırı Tespit Sistemi Genel Görünüm

Bir saldırı tespit sistemi Şekil 2.1'de görüleceği üzere internetten gelen ve sırayla yönlendirici (router) ve güvenlik duvarından geçen trafiğin yerel ağa girmeden önce bir kez daha kontrol edildiği bir durak noktasıdır. Güvenlik duvarı her ne kadar harici ağdan gelen güvenli olmayan paketleri elese de geçen trafik içerisinde güvenli olmayan paketler olabilir. Saldırı tespit sistemleri güvenlik duvarlarını atlatan paketleri yakalamak için kullanılmaktadır. Saldırı tespit sistemleri için yukarıda verilen gösterim en basit gösterimdir. Oldukça

sıradan bir ağ için verilen gösterim gerçek hayatta ve özellikle büyük ölçekte geçerli değildir. Gerçek hayatta bir ağda sadece bir adet STS sistemi değil birden çok STS sistemi bulunur. Onlardan birisi yerel ağ ile aradaki trafiği denetlerken bir diğeri güvenli bölge olarak da adlandırılan ve sunucuların bulunduğu bölgeye giden ağı denetleyen STS sistemidir. Ağın büyüklüğü ve verinin hassasiyetine göre sıklıkla çoklu STS sistemleri kullanılmaktadır.

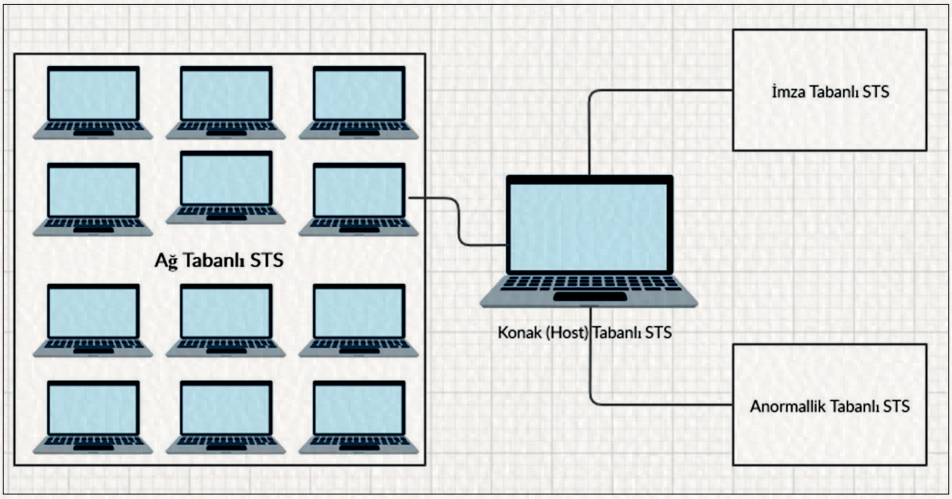
Saldırı tespit sistemleri 1980'li yıllardan bu yana artan bir karmaşıklık derecesi ile gelişim göstermektedir. Saldırı tespit sistemleri öncelikli olarak araştırma maksatlı ele alınmıştır. Bu dönemde yapılan çalışmalar daha çok konak (host) tabanlı saldırı tespiti ile ilgilidir. Konak tabanlı tespit işleminde de analiz edilen veriler işletim sistemi verileri olup analiz yöntemi daha çok örüntü eşleme (pattern matching) yöntemleri şeklindeydi. Sonraki yıllarda konak tabanlı saldırı tespit sistemleriyle birlikte ağ tabanlı sistemler de geliştirilmiştir. İnternet kullanımının yoğunlaşmasıyla birlikte güvenlik duvarları konusunda standartlaşma çalışmaları hız kazanmış ve bu dönemde saldırı tespit sistemleri güvenlik duvarlarına ağın gözlenmesi anlamında yardımcı olmaya başlamıştır. 1990'lı yıllarda konak tabanlı ve ağ tabanlı sistemler bir araya gelerek melez sistemler geliştirilmiştir [6].

Saldırı tespit sistemlerinin amacı saldırıyı engellemek değil saldırı hakkında bilgi toplamaktır. Saldırı tespit sistemleri gerçek hayattaki alarm sistemlerine benzemekle birlikte alarm sistemlerinden en önemli farkı saldırı esnasında tepki vermeyip saldırı sonrası için bilgi toplamasıdır [7]. Bu kapsamda ağ veya sistemlere karşı kötü niyetli bir girişim yakalandığında veya şüpheli bir durum oluştuğunda bu durum ya sistem yöneticine ya da adına SIEM **(**Security Information and Event Management**)** dediğimiz sisteme bildirilir. SIEM sistemine gelen bildirimler bazen hatalı bazen de doğru alarmlar olabilir. SIEM bu alarmların hangisinin hatalı hangisinin doğru olduğunu analiz etmekle yükümlüdür. Bir girişimin saldırı olarak etiketlenebilmesi için, kaynakların uygun olmayan veya hatalı kullanımlarının neler olduğu bilinmelidir. Bir ağ için normal veya normal olmayan girişimler organizasyonun güvenlik politikası tarafından belirlenir [8]. Dolayısıyla diğer güvenlik faaliyetlerinin başarısı gibi saldırı tespitinin başarısı da güvenlik politikalarına bağlıdır.

Saldırı tespit sistemleri güvenlik politikası dokümanında sınırları verilen saldırıların yapılıp yapılmadığını tespit ederek güvenlik uzmanlarına konuyla ilgili bilgilendirmede bulunur. Güvenlik uzmanı veya sistem yetkilisi de gerekli tedbirleri almaktan sorumludur. Yapılan bir işlemin saldırı olup olma-

masıyla ilgili olarak üretilen alarm kimi zaman hatalı olabilmektedir. Saldırı tespit sistemlerinin amacı hatalı alarm oranlarının düşürülmesidir.

Saldırı tespit sistemleri için önemli bir ayrım da saldırı tespit sisteminin çalışma mantığı veya yerleşimiyle ilgilidir. Aşağıda bir bütün olarak saldırı tespit sistemleri için hem yerleşim hem de analiz türüne göre bir gösterim sunulmuştur.



Şekil 2.2. Konak tabanlı ve ağ tabanlı saldırı tespit sistemi

Şekil 2.2'de hem yerleşime dayalı olarak hem de analize dayalı olarak saldırı tespit sistemleri bir arada sunulmuştur. Şekilden de görüleceği üzere ağ üzerindeki bütün cihazlar için saldırı tespitini yerine getiren sistemlere ağ tabanlı STS adı verilmektedir. Ağ içerisinden bir cihazın seçilerek o cihaz üzerinde yapılan derinlemesine analiz ise konak tabanlı STS olarak bilinmektedir. İmza tabanlı STS ve anormallik tabanlı STS ise verinin analiz şekliyle ilgili ayrımı sunmaktadır. Her ne kadar Şekil 2.2'de her iki analiz yöntemi de konak tabanlı saldırı tespit sistemine bağlanmış olsa bile bu yöntemler ağ tabanlı STS için de kullanılabilir sistemlerdir.

2.2.1. Host Tabanlı Saldırı Tespiti

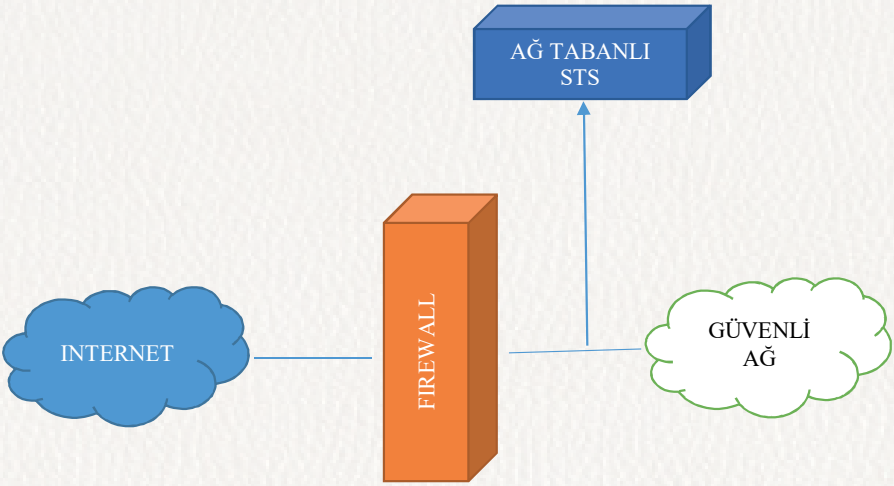
Konak tabanlı bir saldırı tespit sistemi ürünü, ağ ortamında yer alan bir bilgisayar sisteminde çalışan bir yazılımdan ibarettir. Örnek olarak, bir web sunucusunda veya herhangi bir uygulama sunucusunda kurulmuş bir saldırı tespit

sistemi verilebilir. Bu sistemler, sunuculardaki uygulama ve işletim sistemi kayıtlarını takip ederek ilgili analizleri yaparlar. Sunucu tabanlı saldırı tespit sistemleri esas olarak içeriden gelecek tehditlere karşı çok etkilidir. Yetkisiz kullanıcıların, hakkı olmayan ağ kaynaklarına erişim denemeleri bu yolla takip edilir ve gerekli önlemler alınır.

Eğer STS bir bilgisayar sistemi üzerindeki aktiviteleri izleyerek saldırı tespiti yapıyorsa buna Konak tabanlı STS adı verilir. Konak tabanlı STS genellikle web sunucu ve sistem günlük (LOG) dosyaları ile çalışır. İşletim sistemi veya uygulama günlükleri istatistiksel veya buna benzer yöntemlerle analiz edilerek saldırı girişimleri tespit edilir. Konak tabanlı STS her bir cihaz veya makinede ayrı ayrı çalışır ve her makine kendi başına kontrol edilir. Kontrol yöntemi olarak da sistemde bulunan dosyaların o anki durumları alınır ve önceki durumları ile kıyaslanır. Bu kıyaslama sonrasında özellikle de kritik sistem dosyalarında değişiklik veya silinme gibi bir durum gözlenirse alarm oluşturulur [9].

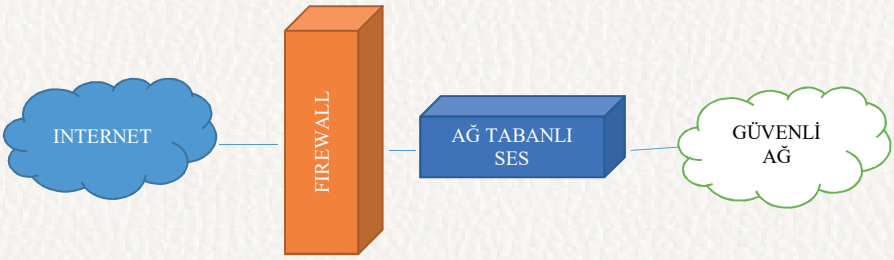
2.2.2. Ağ Tabanlı Saldırı Tespiti

Ağ tabanlı bir saldırı tespit sistemi ürünü, bağımsız bir bilgisayar veya özel tahsis edilmiş bir cihaz üzerinde çalışır ve ağ üzerindeki veri trafiğinin tamamını denetleyip analiz yapar. Bu şekilde işletilen saldırı tespit sistemi ürünleri, kurulu oldukları sistemlerde 'promiscuous' modda çalışıp ağ veya ağın bir parçasından geçen bütün paketleri kontrol ederler. Ağ tabanlı saldırı tespit sistemleri, ağ üzerinde yer alan cihazlardan geçen trafiği pasif olarak dinleyen ve saldırı veya anormal bir durum gözlediğinde alarm üreten yazılım veya donanımlardır [10]. Güvenlik duvarına yetkisiz erişim yapılıp yapılmadığını algılayabilmek için ağ tabanlı STS güvenlik duvarlarının bulunduğu iç ağa kurulmalı ve trafiğin tamamını dinlemelidir. Ağ tabanlı saldırı tespit sistemleri algılama sırasında veri paketlerini analiz eder ve ağ üzerinden akan paketler içerisinde bir imza arar. Ağ tabanlı saldırı tespit sistemleri konak tabanlı saldırı tespit sistemlerinin aksine bireysel dinleme yerine ağın tamamını dinler. Ağ tabanlı saldırı tespit sistemi ağdaki trafiği dinlerken ağı yavaşlatmasın diye kimi zaman OPNET veya Netsim gibi benzetim yazılımları tercih edilir [11]. Ağ tabanlı saldırı tespit sistemleri bazen çevrimiçi bazen de çevrimdışı analiz yaparlar. Bunlara da çevrimiçi STS ve çevrimdışı STS adı verilir.



Şekil 2.3. Ağ tabanlı saldırı tespit sistemi

Ağ tabanlı saldırı tespit sistemleri pasif cihazlardır. Şekil 2.3'te de görüleceği üzere güvenli ağ ile güvenlik duvarı arasındaki akış sadece dinlenir. Ağ tabanlı saldırı tespit sistemleri ağ üzerindeki aktiviteleri izler fakat engelleme yapmaz. Saldırı tespit sistemlerinin temel amacı tanımlanan kurallar çerçevesinde yapılan saldırıları tespit ederek mail veya sms gibi yöntemlerle sistem yöneticisine veya SIEM sistemine haber vermektir. Saldırı tespit sistemlerinin saldırıları engellemek gibi bir görevi yoktur. Bu görevi yerine getiren sistemlere saldırı engelleme sistemleri adı verilir [12]. Ağ tabanlı saldırı engelleme sistemi saldırı tespit sisteminin aksine pasif eleman değil aktif eleman olarak görev yapar.



Şekil 2.4. Ağ tabanlı saldırı engelleme sistemi

Şekil 2.4'te verilen ağ tabanlı saldırı engelleme sistemi saldırı tespit sistemlerinin aksine güvenli ağ ile güvenlik duvarı arasında bir bariyer oluşturur ve güvenli görmediği akışı filtre ederler.

Saldırı tespit sistemleri modern güvenlik uygulamalarının bir parçasıdır. Saldırı tespit sistemleri izleme verileri içerisinden özellikler çıkararak kurallara göre saldırı girişimlerini bulmak için kullanılır. Saldırı tespit sistemleri yaklaşım türüne uygun verilerle çalışır. Örneğin, ağ tabanlı bir saldırı tespit sisteminde saldırı tespiti yapılacak veri ağ üzerinde akan trafik verisidir. Bu verileri elde etmenin en kolay yolu "tcpdump" uygulamasıdır. Eğer konak tabanlı saldırı tespiti yapılacaksa o zaman saldırı tespit verisi "Shell" komut dizileri veya "system calls" bilgileri olacaktır. Yine aynı şekilde konak tabanlı bir saldırı tespit sisteminde işletim sistemi günlükleri kullanılacaktır. Kimi zaman da dağıtılmış yapıda bir ağ üzerinde saldırı tespiti yapılmaya çalışılmakta ve merkeze bağlı algılayıcılardan gelen veriler saldırı tespiti amacıyla kullanılmaktadır.

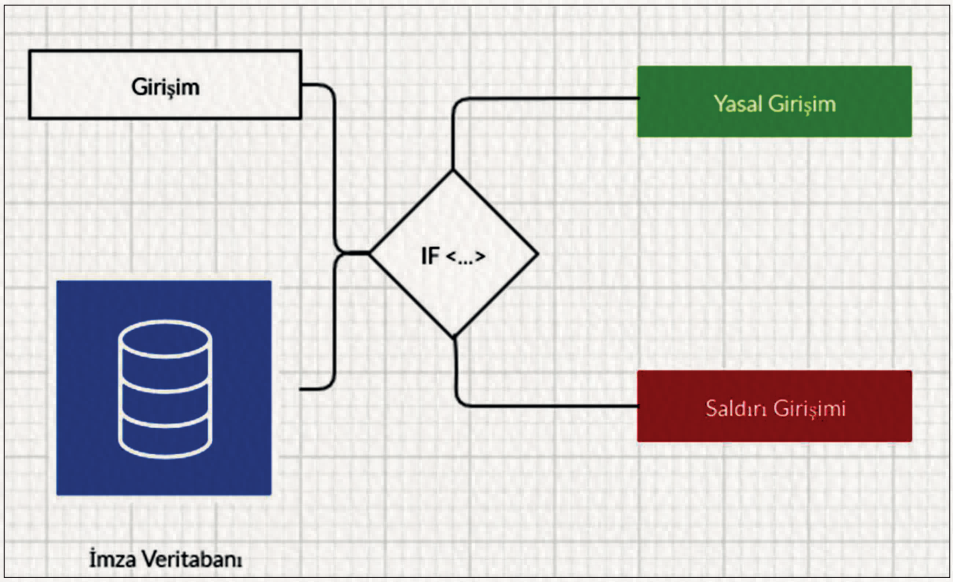
Saldırı Tespit Sistemleri için toplanan veriler genel olarak denetim verisi olarak isimlendirilir. Ayrıca her STS için denetim verisi toplama önemli bir görevdir. Bu veriler saldırı tespit sisteminin yerleşimine ve kullandığı yaklaşıma göre değişiklikler gösterebilir. Saldırı tespit sistemleri tarafından toplanan veriler hem kanıt amaçlı hem de yeni saldırı tiplerinin bulunması açısından önem arz etmektedir. Saldırılarla ilgili veri toplamak önemli olduğu için saldırı tespit sistemleri Honeypot adı verilen bir çözüm ile saldırı verileri toplayıp onları analiz imkânı bulabilmektedir [14]. Son zamanlarda saldırı tiplerindeki artış saldırı tespitini karmaşık bir iş hâline getirmiştir. O yüzden denetim verilerinden saldırı tespiti için güçlü ve zeki veri analiz araçlarına ihtiyaç duyulmaktadır. Veri analizi için kullanılabilecek araçlardan biri ise hiç şüphesiz veri madenciliğidir.

2.3. SALDIRI TESPİTİNDE KULLANILAN YÖNTEMLER

Saldırı Tespit Sistemleri analiz ettikleri verilere dayalı olarak temelde iki kategoriye ayrılır: imza tabanlı ve anormallik tabanlı. Bu bölümde imza tabanlı ve anormallik tabanlı yöntemlerle ilgili detaylar verilecektir.

2.3.1. İmza Tabanlı Saldırı Tespiti

İmza tabanlı saldırı tespitinin çalışma prensibi şöyledir. Sisteme ilk kez yapılan saldırılar analiz edilerek etiketlenir ve etiketli olarak kayıt altına alınır. Ardından yeni bir girişim meydana geldiğinde sistem o girişimi eldeki saldırı örüntüsü ile karşılaştırır ve ona göre karar verir. İlk dönem geliştirilen konak tabanlı saldırı tespit sistemlerinin mantığı imza tabanlıdır. İmza tabanlı yöntem ilk kez meydana gelen saldırıları tanıyamaz fakat daha önce meydana gelen saldırıları hızlıca tanıyabilir. İmza tabanlı saldırı tespitinin sorunlarını gidermek için makine öğrenmesi yöntemlerinin kullanımı bir seçenektir. Böylece ilk kez meydana gelen saldırılar da tanınabilecektir [13]. İmza tabanlı yöntem kimi yerde suiistimal tespiti olarak da bilinir. Kötüye kullanım tespitinde daha çok dâhili ağ kaynaklarına yapılan saldırılar açıklanır.



Şekil 2.5. İmza tabanlı saldırı tespit sistemi genel görünüm

İmza tabanlı saldırı tespit sistemleri daha önceden bilinen bir saldırıyı tespitte örüntü eşleme yöntemlerini kullanır. Örüntü eşleme için bilgi tabanlı (knowledge based) ve hatalı kullanım tespiti (misuse detection) gibi yöntemler bulunmaktadır [15]. Saldırı imzaları belirli bir ihlale ait bütün olasılıkları içinde barındıran bir özet bilgi olarak düşünülebilir. Bu bilginin sunumu genellikle

bir kural şeklindedir. Bu kurallar imza veri tabanı adı verilen bir depoda tutulur ve kullanıcıların sistemi kullanma örüntüleri ile saldırı imzaları arasında bir eşleşme olduğunda sistem tarafından bir alarm üretilir. Saldırı veri tabanında bulunan imzalar daha önceden bir saldırı girişimi olduğu kesinleşen girişim örüntüleridir. Kötüye kullanım tespiti daha fazla uzman bilgisi gerektirdiği için ilk yıllarda fazla bir gelişim gösterememiştir fakat daha sonra konu uzmanlarının artması ile birlikte ticari STS yazılımlarında sıklıkla tercih edilen yöntem olmuştur.

İmza tabanlı saldırı tespit yöntemi bilinen saldırı girişimlerini çok yüksek bir doğrulukla tespit ederken [16] saldırı veri tabanında imzası olmayan sıfır gün ataklarını tespitte başarısız olmaktadır. Bu yaklaşımı kullanan ürünler saldırı veri tabanlarını sıklıkla güncellemek zorunda kalırlar. Dolayısıyla güncelleme masrafı oldukça yüksek bir yöntemdir. Özellikle daha önce meydana gelmiş saldırılar konusunda yöntemin tanıma oranı oldukça yüksektir. Hem doğru tanıma oranı hem de tanıma hızı yüksek olan yöntemin bir dezavantajı ilk kez meydana gelmiş saldırıları tanıma konusundaki yetersizliğidir. İmza tabanlı saldırı tespiti, Snort [17] ve NetSTAT [18] gibi çok sayıda yaygın araçta kullanılmaktadır. Sıfır gün saldırılarının artan oranı [19] imza tabanlı saldırı tespit tekniklerini giderek daha az etkili hâle getirmiştir. Bu soruna potansiyel bir çözüm anormallik tabanlı saldırı tespitinin uygulanmasıdır.

2.3.2. Anormallik Tabanlı Saldırı Tespiti

İmza tabanlı saldırı tespitinin özellikle sıfır gün atakları konusunda başarısız olması ilgiyi anormallik tabanlı saldırı tespitine toplamıştır. Anormallik tabanlı saldırı tespitinin gerisindeki teorik alt yapı saldırıların genellikle olağan dışı eylemler içermesidir. Bir şeyin olağan dışı olduğunun tespiti için de ihtiyaç duyulan önemli bir çalışma sistemin eğitimi olacaktır. Bu eğitim sırasında kaynaklar (kullanıcılar, programlar, sistemler vb.) hakkında veri toplanarak bu verilerden her bir kaynağın normal durumu istatistiksel yöntemlerle tespit edilir ve bu bilgilerden profil adı verilen özet bilgiler elde edilir. Kaynakların davranışlarındaki değişimler düzenli olarak incelenerek profillerin güncellenmesi sağlanır. Profil için genel kabul olarak kaynakların normal şartlar altındaki kullanımlarının bir ortalamasıdır diyebiliriz. Kaynakların kullanımı sırasında kimi zaman anormallikler meydana gelebilmektedir. Ağ trafiğinin aniden yoğunlaşması, bilgisayar sistem kaynaklarının maksimum kullanım

oranlarına çıkması gibi durumlar genellikle anormal durumlardır. Anormal durumlar, genellikle bir saldırı girişimine paralel olarak meydana gelir. Bu motivasyondan yola çıkılarak saldırı girişimlerini tespit etmek için anormal durumların tespiti makul bir yöntem olmaktadır. O yüzden ağ veya bilgisayar sistemlerinde meydana gelen anormalliklerin tespiti saldırı tespitinin en önemli yöntemlerinden birisidir. Normalden belirgin şekildeki sapmalar saldırı girişimi olarak tespit edilir.

Anormallik tespiti yöntemi imza tabanlı yöntemden farklı olarak saldırı imzaları ile değil normal profilden sapmalarla çalışır. Bu nedenle uzmanlık bilgisi gerektirmeyen ama verilerden eğitim gerektiren bir uygulama türüdür. İmza tabanlı yöntemlerde olmayıp da anormallik tabanlı yöntemlerde olan bir özellik yeni saldırı girişimlerinin tespit edilebilmesidir. Bu yönüyle denetimsiz öğrenme tekniğinden de faydalanmaktadır. Bu yöntemin en büyük dezavantajı çok sayıda hatalı alarm üretmesidir. Hatalı alarm sayılarının artmasının en önemli nedeni normal durumu karakterize eden profilin bulunmasının zorluğudur. Anormallik tabanlı saldırı tespiti konusunda çok sayıda çalışma olup saldırı tespiti teknikleri arasında öne çıkan tekniktir. Bu nedenle anormallik tespiti kullanan yöntemleri kendi içerisinde aşağıdaki kırılımlar şeklinde sunmak uygun olacaktır.

i. İstatistiksel anormallik tespiti

İstatistik tabanlı saldırı tespit sistemleri normal davranış profili için bir dağılım modeli inşa ederek bu dağılımdan sapmaları potansiyel saldırılar olarak etiketler. İstatistiksel sistemler paketlerdeki sapmaları mod, medyan, standart sapma gibi istatistiksel ölçümler olarak ele alır. Bir şeyin saldırı olduğunu tespit edebilmek için neyin normal olduğunun bulunması bir ihtiyaçtır. İstatistik tabanlı anormallik tespiti kendi içerisinde tek değişkenli, çok değişkenli ve zaman serileri modeli şeklinde alt türlerden oluşur. Tek değişkenli STS her bir metrik için ayrı ayrı anormallik arayan yöntemi ifade ederken çok değişkenli STS aynı anda birden çok değişkenin etkisinden anormallik bulmaya odaklanmıştır [20]. Zaman serisi analizi ise belirli bir zaman aralığında bir dizi gözlem yapmaya dayalıdır.

ii. Bilgi tabanlı anormallik tespiti

Bilgi tabanlı anormallik tespiti uzman sistem yardımıyla saldırı tespiti olarak da görülebilir. Normal olan girişimlerin tamamının kural şeklinde bir karşı-

lığı vardır. Normal olmayan bir girişim eldeki kuralların kontrolü şeklinde meydana gelir. Kural kümesinde olmayan bir girişim anormal bir girişimdir. Bu teknik eldeki kurallar dâhilinde hızlı sonuç verir. Bununla birlikte kural kümesinin güncellenmeye ihtiyacı vardır [11].

iii. Makine öğrenmesi tabanlı anormallik tespiti

Makine öğrenmesinde çözülen problemlerden birisi anormal durumların tespitidir. Örneğin, temel makine öğrenmesi ve istatistik operasyonlarından birisi sapma bulmadır (outlier detection). Ayrıca son zamanlarda önemi iyice artan makine öğrenmesi uygulamalarından birisi istisna saptanmasıdır (fraud detection).

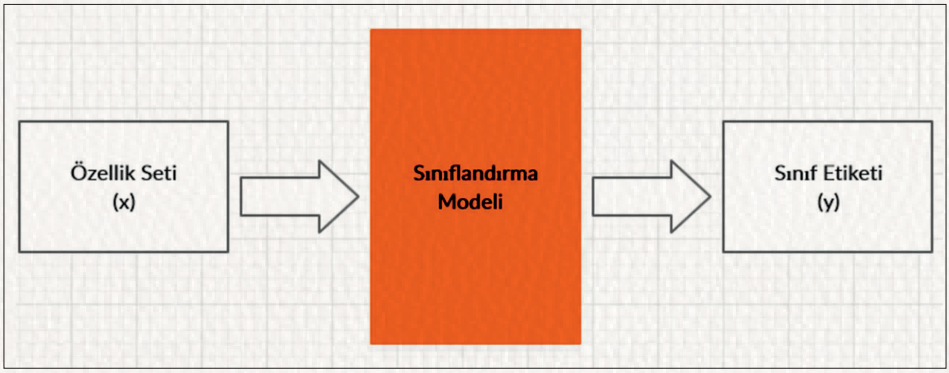
Makine öğrenmesi teknikleri veriler içerisinden kalıplar, kurallar ve bilgi parçaları bulmaya odaklanmış analitik yöntemleri içerir. Makine öğrenmesi teknikleri anormallik tespitinde yaygın olarak kullanılmaktadır. Örneğin, kümeleme analizi, yapay sinir ağları, ilişkilendirme kuralları, karar ağaçları, genetik algoritmalar ve en yakın komşu yöntemleri gibi çeşitli algoritmalar nüfuz veri kümelerinden bilgiyi keşfetmek için uygulanmıştır [21] [22]. Chebrolu ve arkadaşları Bayesian ağları ve sınıflandırma regresyon ağaçları algoritmalarını iki farklı özellik setiyle birlikte kullanmış ayrıca daha yüksek doğruluk için iki yöntemi birleştirmişlerdir [23].

Saldırı tespitinin makine öğrenmesi teknikleriyle yerine getirilmesinin önemli bir nedeni ilk kez meydana gelen saldırı girişimlerini yakalama kapasitesinin olmasıdır. Makine öğrenmesi tekniklerinden birisi olan kümeleme sayesinde ilk kez meydana gelen bir durum tanınabilmektedir. Temel felsefesi kullanıcıları genel özelliklerine dayalı olarak gruplara ayırmak olan kümeleme [24] tekniği denetimsiz bir teknik olup genelleştirme yeteneklerini içermektedir. Saldırı tespitinde makine öğrenmesi teknikleri kullanımının diğer sebepleri şunlardır:

- Denetim (audit) verisi üzerinde normal girişimler ve saldırı girişimleri delil bırakırlar. Bu deliller makine öğrenmesi gibi deneyimlerden öğrenen yöntemler ile analiz edilebilir.
- Veriye dayalı bakışla saldırı girişimlerinin tespiti bir veri analiz görevidir. Ayrıca, günlük verilerinin dönüşümü, onların görselleştirilmesi ve diğer yetenekler için de makine öğrenmesi bir ihtiyaçtır.

- Saldırı tespiti, kredi kartı yolsuzluklarının tespiti ve hatalı alarmların yönetimi gibi uygulamalarla aynı etki alanı içerisindedir.
- Bugüne kadar denetim verilerine uygulanan makine öğrenmesi algoritmaları sınıflandırma, link analizi ve sıralı analiz olmuştur [10]. Bununla birlikte diğer birçok veri madenciliği ve makine öğrenmesi tekniği de saldırı tespiti için faydalı özellikler içermektedir.

a. Denetimli öğrenim teknikleri yardımıyla anormallik tabanlı saldırı tespiti



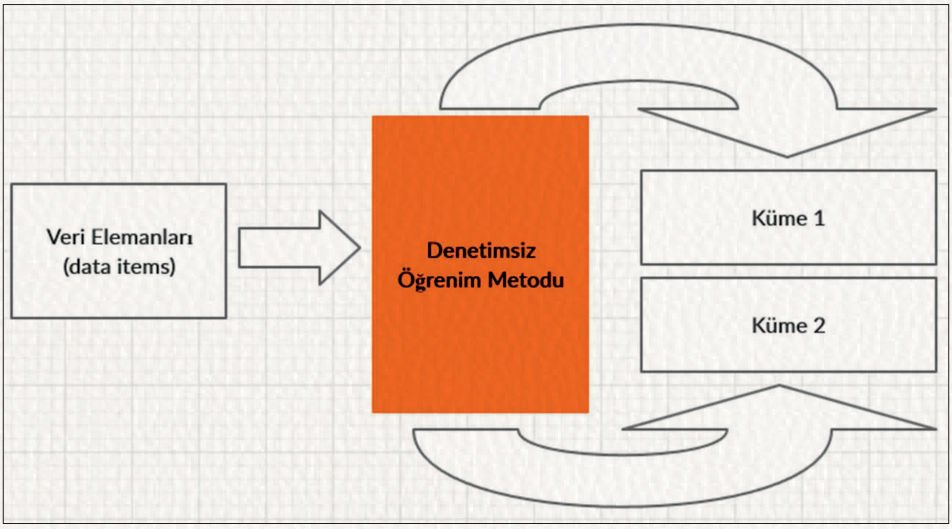
Şekil 2.6. Denetimli öğrenim tekniğinin genel görünümü

Saldırı tespitinde makine öğrenmesi teknikleri kullanımında öne çıkan teknikler denetimli öğrenim teknikleridir. Tahminsel modeller olarak da bilinen bu tekniklerden en fazla öne çıkanı sınıflandırma algoritmaları olmuştur. Sınıflandırma algoritmaları önceden belirlenmiş kategorilere yeni veri elemanlarının atanması ile ilgili olduğundan özellikle çoklu sınıflayıcılar ile farklı tipteki saldırı girişimlerinin tespit edilmesi mümkün olabilmektedir. Her bir saldırı sınıfı eğitim verisiyle eğitilerek yeni gelen girişimlerin hangi saldırı türüne ait olduğu bulunabilir. Ya da bir girişimin saldırı olup olmadığı sınıflandırma algoritmalarıyla bulunabilir. İki durumlu sınıflayıcılar ile saldırı tespiti esnasında normal girişimler modellenir ve normal girişimlerden sapmalar saldırı olarak etiketlenir.

Bir denetimli öğrenme süreci temel olarak eğitim ve test gibi iki adımdan oluşur. Eğitim aşamasında seçilen özellikler ve seçilen kategorilere dayalı olarak erişim verilerinden model inşa edilir. Model inşası sırasında tercih edilen

makine öğrenmesi algoritmasının ne olduğu önem kazanmaktadır. Eğer seçilen makine öğrenmesi algoritması yapay sinir ağları ise karşımıza öğrenilmiş ağırlıklar, seçilen bir karar ağacı ise karşımıza karar destek amaçlı bir ağaç çıkacaktır. Eğitim sırasında önemli bir konu özellik seçimidir. Hangi özelliklerin diğerlerinden daha değerli olduğunu özellik seçimi yardımıyla görebiliriz. Model oluşturulduktan sonra en son aşamada test veya sınıflandırma işlemine geçilir. Sınıflandırmanın sonucu ağ veya bilgisayar sistemine yapılan girişimin saldırı olup olmadığı belirlenir.

b. Denetimsiz öğrenim teknikleri yardımıyla anormallik tabanlı saldırı tespiti



Şekil 2.7. Denetimsiz öğrenim algoritmaları genel görünüm

Kümeleme tekniği verilerin, benzer özellikler taşıyanlarının bir arada gruplandığı bir teknik olduğundan daha önceden bilinmeyen saldırı girişimleri bilinen saldırı girişimlerine benzerliklerine göre tespit edilebilirler. Kümeleme tekniğini saldırı tespitinde sınıflandırma tekniğinden daha önemli hâle getiren durum ise kümeleme tekniği sayesinde ilk kez meydana gelmiş saldırı girişimleri de tanınabilmektedir.

Denetimsiz teknikler bağlamında diğer önemli algoritma birliktelik kuralları madenciliğidir. Birliktelik kuralları madenciliği veri tabanlarında yer alan

nesneler arasındaki ilişkilerin tarandığı bir yöntemdir. Veri tabanındaki bütün ilişkiler güven ve destek sınırları içerisinde ortaya çıkarılır. Birliktelik kuralları sayesinde farklı saldırı girişimleri arasındaki eşleşmeler bulunabilir. Birliktelik kurallarının devamı niteliğindeki sıralı örüntü analiz tekniği de belli bir sıraya göre yapılan saldırı girişimlerini tespit konusunda kullanılmaktadır.

c. **Yarı denetimli öğrenim teknikleri yardımıyla anormallik tabanlı saldırı tespiti**

Son dönemde gündemimize girmeye başlayan yarı denetimli tekniklerde de sınıfı bilinen çok az sayıda örnek ile sınıfı bilinmeyen örnekler hakkında hüküm verme imkânları artmaya başlamıştır. Makine öğrenmesinin denetim verilerine uygulanması sonucunda Saldırı Tespit Sistemleri için kurallar bulmak, daha önceden bilinmeyen saldırı girişimleri için imzalar keşfetmek ve paralel saldırı girişimlerini tespit etmek mümkün olacaktır.

2.4. VERİ MADENCİLİĞİ İLE SALDIRI TESPİTİ

Saldırı tespit sistemlerinde kullanılan yöntemlerin avantaj ve dezavantajları bulunmaktadır. Bu tür durumlarda avantajı maksimize edecek akıllı veri analiz yöntemlerine ihtiyaç vardır. Veri madenciliği bu anlamda değerlidir. Veri madenciliği; büyük miktardaki veriden anlamlı ve gizli kalmış bilgilerin açığa çıkarıldığı bir yöntemdir. Veri madenciliği yaklaşımı ajan tabanlı bir yaklaşım olup öğrenim ve tespit ajanları bulunmaktadır. Öğrenim ajanları tümevarım yöntemiyle devamlı eğitilirken, tespit ajanları saldırı girişimlerinin tespiti için güncellenmiş modeller sunarlar. Veri madenciliği disiplini bir taraftan istatistik teknikleri diğer taraftan makine öğrenmesi yöntemlerini kapsar. Dolayısıyla eğer bir çözümde veri analitiği anlamındaki tekniklerin tamamı bir çatı altında kullanılacaksa ortaya konacak çözüm bir veri madenciliği çözümü olacaktır.

Veri madenciliğinin saldırı verilerine uygulandığı yönteme denetim verilerinin madenciliği adı verilmektedir. Denetim verilerinin madenciliği için sınıflandırma, kümeleme ve birliktelik kuralları gibi temel veri madenciliği yöntemleri uygulanmaktadır.

Denetim verilerine uygulanan veri madenciliği algoritmaları ile faydalı bir dizi bilgiyi bulmak mümkündür. Veri madenciliğinin artan önemi veri madenciliği ile yerine getirilen uygulamaların sayısını arttırmıştır. Bunlardan birisi

de veri madenciliğinin web verilerine uygulandığı web madenciliğidir. Web madenciliği için bugüne kadar çok sayıda tanım yapılmıştır ama en kaba tanımıyla web madenciliği webden faydalı bilginin keşfedilmesi olarak tarif edilebilir [25]. Web birbirinden farklı üç tür veri tutar. Bunlardan ilki içerik verisi (web content data), ikincisi yapı verisi (web structure data) diğeri ise kullanım verisidir (web usage data). Bu verilerle ilintili olarak web madenciliğinin üç alanı otaya çıkmıştır. Bu alt alanlar web sitesinin yapısı ile ilgili analizi içeren web yapı madenciliği, web sitesi içerisinde yer alan verilerin analizini içeren web içerik madenciliği ve web sunuculardan kullanıcı erişim örüntülerinin keşfi ve analizinde kullanılan web kullanım madenciliğidir [26].

2.4.1. Saldırı Tespit Sistemleri ve Web Kullanım Madenciliği

Web kullanım madenciliği; web sunucularından kullanıcı erişim örüntülerinin analizinin yapıldığı bir tip veri madenciliği uygulamasıdır. Web kullanım madenciliği kimi yerde web günlük (log) madenciliği adıyla da anılır. Web günlük madenciliği adını almasının nedeni web kullanım madenciliği esnasında kullanılan verilerin günlük verileri olmasıdır. Web günlük verileri web sunucuları üzerinde yapılan her türlü etkinliğe dair bilgi tutar. Günlük dosyalarında, kullanıcı tarafından istenen her sayfa günlük dosyasında bir kayıt olarak tutulur [27].

Web kullanım madenciliği yardımıyla yapılan işlemler güvenlik sistemlerinde önemli bir görev olan log tutma, log izleme ve log denetimi ile doğrudan ilişkilidir. Log kayıtları kritik ağların, cihazların ve sistemlerin ürettiği olay kayıtlarından oluşur. Bilişim sistemleri tarafından üretilen olay kayıtlarının izlenmesi ve analiz edilmesi ise log izleme olarak bilinir. Bu yönüyle log izleme saldırı tespit sistemlerinde tanımlayama çalıştığımız göreve oldukça yakın bir işleve sahiptir. Toplanan log verileri üzerinde yapılacak veri önişlem faaliyetleri (toplama, birleştirme, dönüştürme vs.), log verilerinin metin analiz dâhil olmak üzere analiz edilmesi ve log verilerinden çıkarılan bilgilerin sunumu log yönetimi adını almaktadır. Log yönetimi sayesinde saldırıya ait delillerin ortaya çıkarılması imkânı oluşmaktadır. İdeal log yönetimi canlı olarak logların analiz edilmesidir. Bununla birlikte mevcut sistemlerin önemli bir kısmı bu faaliyeti çevrimdışı olarak yerine getirmektedir.

Log dosyalarında tutulan olay kayıtları aslında denetim (audit) maksadıyla kayıt altına alınmaktadır. Bu verilerin analizi ile sadece saldırı girişimlerinin

fark edilmesi değil aynı zamanda ziyaretçilerin bir web sitesinde ne kadar vakit geçirdiği, firmanın hizmet stratejileri, kampanya bilgileri ve benzer bilgiler bulunabilir. Ayrıca siteye bağlanan kullanıcıların hangi niyetle bağlandığı, kötü niyetli olup olmadıkları tespit edilebilir. Güvenlik maksatlı log izleme kadar güvenlik harici log izleme de bugüne kadar yapılmıştır. Dolayısıyla burada güvenlik kapsamından bağımsız olarak log madenciliği konusunun detayları ortaya çıkarılıp sonra güvenlik bağlamı ile ilişki kurulacaktır.

Web kullanım madenciliği bir süreç olarak; web günlük dosyalarında yer alan verilerden anlamlı bilgi çıkarmayı sağlayan adımlar topluluğudur. Diğer veri madenciliği süreçleri gibi veri temizleme, dönüşüm, örüntü keşfi ve analizi aşamalarından oluşmaktadır. Web kullanım madenciliği açısından temizleme log verisi içerisinde yer alan gereksiz ve ilişkisiz bölümlerin veriden çıkarılmasıdır. Dönüşüm aşamasında ise veriler kullanıcı tabanlı, sayfa tabanlı, tuş akışı tabanlı, oturum tabanlı şeklinde özetlenir. Örüntü keşfi aşamasında temizleme ve dönüşümden geçirilen veriler üzerinde; temel veri madenciliği algoritmaları uygulanabilir. Sınıflandırma, kümeleme, birliktelik kuralları madenciliği bu kapsamda en sık kullanılan yöntemlerdir. Ayrıca bilgi sorgulama ve OLAP işlemleri yardımıyla da analiz yapılabilmektedir [28].

2.4.2. Web Miner Tasarımı

Web Miner bir ürün adı değil web üzerindeki verileri analiz eden ve bundan anlamlı bilgiler elde eden uygulamaların genel adıdır. Web verilerin çalışılması web kullanımının yaygınlaşması ile birlikte bir zorunluluk hâline gelmiştir. Toplanan bol miktardaki veri işletmeler için değerli bilgiler barındırmaktadır. Bu veriler genellikle sunucu günlüklerinde tutulur [29]. Web sunucu günlüklerinin keşif ve analizi ile değerli bilgiler elde edilebilecektir.

Web Miner tasarımı konusunda örnek bir çalışma GYTE (Gebze Yüksek Teknoloji Enstitüsü) Kütüphanesi web sitesi için yapılmıştır. Bu çalışmada kütüphane web sitesine yapılan saldırılar web loglarına dayalı olarak tespit edilmeye çalışılmıştır. Web günlüklerine dayalı analiz işleminde veri madenciliği tekniklerinden yararlanılmıştır. Sunucuya yapılan bağlantı ve istek bilgilerini tutan sunucu günlükleri uygulamada analiz edilen verileri oluşturmuştur. Sunucu üzerindeki veriler hangi kütüphanecilik hizmetinin daha sık kullanıldığına dair bilgi verdiği gibi hizmetlere bir saldırı olup olmadığını tespit konusunda da bilgi sağlamıştır. Bu çalışmaya başlarken ortaya koyduğumuz hipotez “sunucuya

yapılan bağlantı sıklıklarının ve sunucudan istenen dosya tiplerinin saldırı tespiti konusunda bilgi verebileceği" temeline dayanmaktadır.

Saldırı tespiti konusunda daha önce de belirtildiği gibi sınıflandırma ve kümeleme gibi temel veri madenciliği teknikleri kullanılabilir. Sınıflandırma algoritmaları sıklıkla kullanılmasına rağmen kümeleme kullanımı saldırı tespitinde daha fazla bilgi verici bir yöntemdir. Kümeleme analizi sayesinde web sunucuya bağlanan kullanıcıların genel karakteristiklerine göre gruplar ayrılması mümkün olabilecektir [24]. Benzer karakteristikler gösteren kullanıcıları kümelemek web kullanım madenciliği açısından değerli bilgiler verecektir. Söz konusu çalışma kümeleme analizi olduğu için saldırı tespiti probleminde bulunması gereken kümelerin ne olduğu söylenmelidir. Bu kümeler kabaca iki tanedir. Kümelerden birisinde saldırı örüntüsü gösteren kullanıcılar diğerinde ise normal davranış gösteren kullanıcılar gruplanmalıdır. Kullanıcıları erişimlerine dayalı olarak gruplayabilmek için de erişimin özelliklerine ihtiyaç vardır. Erişim yapılan dosyaları normal ve anormal şeklinde etiketlemek ve bunları normal olup olmamasına göre puanlamak kullanıcı gruplama için bize imkân sunacaktır. Örneğin, bir kütüphane web sitesinde kişilerin kitap arama gibi bir işlem için istekte bulunmaları normal fakat sunulmayan bir dosyanın istenmesi anormal bir etkinliktir. Sunulmayan bir dosyanın istenmesi web sitesinin taranması gibi bir amaca hizmet etmektedir. Bununla birlikte sayfaların bir oturumda normal kullanımdan çok aşırı fazla istenmesi de bir anormallik işaretidir. Çalışmanın kümeleme yaklaşımları yapılması sayesinde daha önce modeli olmayan saldırılar da bu yaklaşımla gruplanabilecektir [30].

Web siteleri bazen bir hizmet sunmak veya paydaşlara içerik paylaşmak için hizmet verir. Bununla birlikte herkesin kullanımına açık olduğu için saldırılara da açıktır. Bu durum onların bolca saldırıya maruz kalması sonucunu doğurmuştur. Güvenlik duvarları internetten gelecek tehlikeler konusunda bir miktar yardımcı olmakla birlikte 80 numaralı portun açık olması nedeniyle saldırıların tamamını güvenlik duvarı ile engellemek mümkün değildir. Dolayısıyla, güvenlik duvarlarına da yardımcı olabilmek için web günlükleri analiz edilerek otomatik şekilde sistem yöneticisine alarm verilecektir. Böylece web kullanım madenciliği yardımıyla güvenlik için çözüm üretilecektir.

Yaptığımız keşif ve analiz çalışmaları neticesinde önemli bazı bilgiler bulunmuştur. Bunlardan birisi web sitesinden talep edilen dosya türlerinin üç kategoride olmasıdır. Bu kategorilerden birincisi kütüphane web sitesinde

sunulan hizmetlerle ilgili sunucu tabanlı betikler, yani uzantısı .asp olan dosyalardır. Diğer kategori, bir hizmetle ilişkili olmayan, site üzerindeki sabit bilgileri sunan bilgi amaçlı dosyalardır. Bir diğer kategori ise site üzerinde bulunmayan çalışabilir dosya uzantıları ile ilgili isteklerle ilgili kategoridir. Bu kategoride yer alan dosyalar uzantısı .exe veya .dll dosyalar olmuştur. Bu kategoriler bir bilgi sunmakla birlikte bu kategorilerden istenen dosyaların sıklıkları da ek bilgi sunacaktır. Modelimiz dosya kategorileri ve onların sıklığı üzerinden bir puan elde edilmesi ve ona dayalı olarak çıkarım yapılmasıdır.

Yukarıda detayları verilen prensibe göre çalışma yapılmış ve bu çalışmanın bir özeti aşağıdaki tablolarda sunulmuştur. Veriler bu konuda yapılan bir ayrıştırma yazılımından elde edilmiş olup Tablo 2.1'de sunulmuştur.

Tablo 2.1. Kullanıcılar tarafından istenen dosyaların türüne göre sıklıkları

	index.htm	*.asp	*.htm	*.jpg	*.gif	*.exe	*.dll	*.ida	Toplam
User 1	150	170	300	50	65	0	0	0	735
User 2	0	0	0	0	0	1025	180	0	1205
User 3	0	0	0	0	0	850	170	0	1020
User 4	0	0	0		0	660	110	153	923
User 5	77	361	204	141	117	1	0	10	911

Bu veriler yardımıyla puanlama yapıldığında user 2, user 3 ve user 4 isimli kullanıcıların saldırı amaçlı bağlandıkları görülmektedir. Puanlamaya ek olarak yoğunluk testi yardımıyla da ilgili kullanıcıların saldırı amaçlı kullanıcılar, yani saldırganlar olduğu görülmektedir. Erişim sayılarına dayalı hesaplanan rakamlar ile dosya nitelikleri için atanan birim puanların çarpımı ile de yeni bir skor elde edilerek bu yeni puana göre de saldırı tespiti yapılabilecektir. Tablo 2.2 her bir dosya türü için birim puanları Tablo 2.3 ise birim puanlara dayalı toplam puanları vermektedir.

Tablo 2.2. Her bir dosya türü için birim puanlar

index.htm	*.asp	*.htm	*.jpg	*.gif	*.exe	*.dll	*.ida
2	4	2	1	1	-1	-1	-1

Tablo 2.3. Her bir bilgisayar için toplam erişim puanları

	index.htm	*.asp	*.htm	*.jpg	*.gif	*.exe	*.dll	*.ida	Toplam
User 1	300	680	600	50	65	0	0	0	1695
User 2	0	0	0	0	0	-1025	-180	0	-1205
User 3	0	0	0	0	0	-850	-170	0	-1020
User 4	0	0	0	0	0	-660	-110	-153	-923
User 5	154	1444	408	141	117	-1	0	-10	2253

Tablo 2.3 verilerine göre user 1 ve user 5 için elde edilen puanlar sıfırın üzerinde olup benzer davranış göstermiştir. Geriye kalan user 2, user 3 ve user 4 ise kendi arasında benzer bir örüntü vermiştir. Bu temel ayrım haricinde de user 1 isimli kullanıcı user 5 isimli kullanıcıdan daha fazla olumlu davranış gösterdiği gibi olumsuz davranış gösteren diğer kullanıcılar da kendi arasında derecelendirilebilir hâldedir. Başta Tablo 2.3 değerleri olmak üzere elde edilen veriler üzerinden aşağıdaki yorumları yapmak olasıdır.

- Bir web sunucuya yapılan dürüst bağlantılar için her bir oturumdaki ortalama bağlantı sayısı belli iken o ortalamanın oldukça üzerinde yapılan bağlantılar şüphelidir. Ortalamanın çok üzerinde bağlantı yapılması bir saldırı işaretidir.
- Normal kullanımda her bir sayfa için ortalama hizmet süresi belli iken kısa bir sürede aşırı bağlantı niyetin bağlanmak olmadığı tarama olduğu sonucunu doğurur. Bu durum da bir saldırı işaretidir.
- Bir web sunucunun sunmuş olduğu nesneler (sayfalar ve diğerleri) belli iken sayfada olmayan nesnelerin istenmesi bir saldırı işaretidir. Dolayısıyla sistemde sunulmayan dosya içeriklerine negatif puanlar vererek saldırı tespiti yapılabilir.
- Ayrıca, bir sayfaya sıklıkla farklı zamanlarda tek bir istek göndermek de yine bir saldırı işareti olarak ele alınabilir.

Beş adet kullanıcı için örneklenen modele göre sisteme bağlantı yapan bütün kullanıcılar normal ve anormal şeklinde etiketlenerek veritabanımıza kaydedil-

miştir. Kara liste (black list) olarak da görülebilecek bu kayıt işlemi ardından eğer yeniden kara listeden kullanıcılar bağlantı kurmak isterse bunlar otomatik olarak engellenmiştir. Dolayısıyla anormallik tabanlı olarak işaretlenen kullanıcılar bir sonraki ziyaretlerinde suiistimal tespiti yöntemleriyle engellenmiştir. Bu arada kesin karar verilemeyen durumlar ise analiz maksatlı olarak karantinaya alınarak karantinada tutulan veriler üzerinde daha ileri analizler yapılacaktır. Bu analizler neticesinde kesin karar verilenler yine işaretlenir.

Önerdiğimiz bu çalışmada skora dayalı bir çalışma yapılmış ve doğrusal sınıflandırma mantığı ile normal ve anormal aktiviteler işaretlenmiştir. İşaretlenen bu veriler imza veritabanına kayıt edilmiş ve sonraki erişimler için suiistimal tespiti maksadıyla kullanılmıştır. Kullanıcıların doğrusal sınıflayıcı yardımıyla normal ve anormal sınıflarına ayrıldığı gibi daha ileri analizler ile kümeleme yardımıyla da normal ve anormal durumların tespiti mümkün olabilecektir. Kümeleme analizi yardımıyla yapılacak saldırı tespitinde normalin sınırları belirgin olarak çizildikten sonra normalden belirgin olarak sapma gösterenler anormal olarak işaretlenecektir.

Bu çalışmada, web madenciliği alanında öne çıkan ve bugüne kadar öneri sistemlerinde de kullanılan web kullanım madenciliği tekniği saldırı tespiti maksadıyla kullanılmıştır. Web sunucularında bağlantı bilgilerini tutan günlük (log) dosyalarını analizi ile yerine getirilen saldırı tespitinin geri planında skora dayalı doğrusal sınıflandırma vardır. Yapılan çalışma kümeleme analizi tekniklerine de uygun durumdadır. Günlük dosyalarından bilgi çıkarımı ve hesaplama işlemleri için web miner adını verdiğimiz bir uygulama kullanılmıştır.

2.5. SONUÇ VE DEĞERLENDİRMELER

Her geçen gün kurumların ve kişilerin dijitalleşebilen her şeylerini elektronik ortama emanet ettiği bir dünyada güvenlik daha uzun yıllar ve belki de sonsuza kadar konuşulmaya devam edecek ve bu konudaki çalışmalar devam edecektir. Güvenlik artık bir zorunluluktur. Devletler başta olmak üzere her türden ölçekteki firma güvenlik birimi oluşturmalı ve sıkı şekilde güvenlik olaylarını takip etmelidir.

Kişiler ve kurumlar kavram seviyesinde bile olsa bilgi güvenliğini, kapsamını, vereceği zararı, karşılaşılabilecek riskleri bilmelidir. Sistem güvenli-

ği, işletim sistemleri güvenliği veya güvenli işletim sistemi, ağ güvenliği, sunucu güvenliği, GD, virüs ve antivirüs, kurtçuklar, zararlı yazılımlar, şifreleme, parola politikası, GD ve güvenlik politikası gibi terimler bunlardan bazılarıdır.

Saldırı tespit sistemleri bir şekilde güvenlik uygulamalarını atlatarak sisteme yerleşenlerin tespit edilmesine odaklanmış uygulamalara verilen isimdir. Belki de güvenlik etki alanında önemi çok anlaşılmamış ama en önemli konulardan birisidir. Bir düşünün bir saldırgan veya ajan sisteme sızmış ve siz onu fark etmeden ona hizmet ediyorsunuz. Sisteminize girmiş ve kendi emellerini size yaptırıyor. Farkında olmadan zombi olmuş ve sağa sola saldırı yapıyorsunuz. İşte saldırı tespit sistemleri bu türden anormal durumlara düşmemek için kullanılması gereken uygulamalardır. Bu sistem, güvenlik duvarlarının başyardımcısı ve en büyük saldırı kaynağı olan dâhili ağdan gelebilecek tehlikelere karşı bir önlemdir.

Artan saldırılar saldırı tespit sistemlerinin önemini arttıracaktır. Yapay zekâ ve makine öğrenmesi konusunda geliştirilen algoritmalar ve büyük veri imkânları çok daha ileri seviye saldırı tespit sistemlerinin geliştirilmesine yardımcı olacaktır. Son dönemde günlük verilerinin tutulmasıyla ilgili zorunluluk nedeniyle artık günlük verileri üzerinde çalışma imkânları daha fazla olacaktır. Teknolojik imkânlar ile saldırganlardan bir adım öne geçmek mümkün olabilir. Bu konuda yapılacak çok iş olması kimseleri yılgınlığa sürüklemesin. Sorunun olduğu yerde çare de bulunur.

Bu bölümde kısaca anlatılan günlük analizi ile saldırı tespit sistemlerinde veri madenciliği kullanımıyla ilgili bir örnek sunulmuştur. Bu basit örnek sayesinde günlük verilerinin hangi aşamalardan geçtikten sonra analize hazır hâle geldiği, elde edilen bilgilerin ne şekilde kullanıldığı gösterilmiştir. Kullanılan yöntem içerisinde verinin çıkarılması anlamında web günlük madenciliği, puanlama anlamında istatistiksel yöntemler, yorumlama anlamında ise denetimli öğrenme tekniklerinden faydalanılmıştır. Birden fazla çalışma alanının bir arada kullanıldığı bu yöntem aslında melez yöntem olarak görülebilecektir.

Saldırı tespit sistemleri önceleri kötüye kullanım ve anormallik tespiti şeklinde yerine getirilmiş ve zamanla anormallik tespitinde makine öğrenme yöntemleri ağırlık kazanmıştır. Diğer veri analiz yöntemlerinde olduğu gibi saldırı tespit sistemlerindeki analiz yöntemlerinin de güncel algoritmalar ve veri

kaynakları ile zenginleştirilmeye ihtiyacı vardır. Her dönem geliştirilen saldırı tespit sistemleri o dönemin veri analiz teknikleriyle uyumlu olduğu gibi son dönemde geliştirilen saldırı tespit sistemleri de son dönemin veri analiz yöntemlerine uygun olmalıdır.

KAYNAKLAR

1. Dayıoğlu, B. ve Özgit, A. İnternet' de saldırı tespiti teknolojileri, İletişim Teknolojileri 1. Ulusal Sempozyumu ve Fuarı, 17-21 Ekim 2001, Ankara/Türkiye (n.d.).
2. Denning, D. (1986). An Intrusion Detection Model. In Proceedings of the IEEE Security and Privacy Conference.
3. Mukherjee, B., Haberlein, L. T. ve Nevitt, K. N. (1994). Network intrusion detection. IEEE Network, 8(3).
4. Hindy, H., Brosset, D., Bayne, E., Seeam, A., Tachtatzis, C., Atkinson, R.C. ve Bellekens, X.J. (2018). A Taxonomy and Survey of Intrusion Detection System Design Techniques, Network Threats and Datasets. *ArXiv,* abs*/1806.03517*.
5. Axelsson, S (2000). "Intrusion Detection Systems: A Survey and Taxonomy" (retrieved 21 May 2018).
6. Frincke, D. A. ve Ming-Yuh Huang, M.-Y. (2000). Recent advances in intrusion detection systems. Computer Networks, 34, 541–545.
7. Dayıoğlu, B. (n.d.). Elektronik Saldırı Tespiti. Retrieved April 3, 2002, from http://www.teknoturk.org/docking/yazilar/tt000026-yazi.htm
8. Kudyachete, G. (2002). Intrusion Detection Report. University of Pittsburgh.
9. Groom, F. M., Groom, K., & Jones, S. S. (n.d.). *Network and Data Security for Non-Engineers*. CRC Press.
10. Lee, W. ve Stolfo, S. (1998). Data Mining Approaches for Intrusion Detection, Computer Science Department Columbia University.
11. Khraisat, A., Gondal, I., Vamplew, P. *vd.* Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecur* **2,** 20 (2019). https://doi.org/10.1186/s42400-019-0038-7.
12. *Newman, R. (2010). Computer Security: Protecting Digital Resources. Jones & Bartlett Learning.*
13. Eskin E., Arnold A., Prerau M., Portnoy L., Stolfo S. (2002) A Geometric Framework for Unsupervised Anomaly Detection. In: Barbará D., Jajodia S. (eds) Applications of Data Mining in Computer Security. Advances in Information Security, vol 6. Springer, Boston, MA
14. Mohammed, M. ve Rehman, H.-ur. (2015). *Honeypots and Routers: Collecting Internet Attacks*. CRC Press.

15. Khraisat, A., Gondal, I. ve Vamplew, P. (2018). An Anomaly Intrusion Detection System Using C5 Decision Tree Classifier. *Lecture Notes in Computer Science Trends and Applications in Knowledge Discovery and Data Mining*, 149–155. doi: 10.1007/978-3-030-04503-6_14.
16. Kreibich, C. ve Crowcroft, J. (2004). Honeycomb. *ACM SIGCOMM Computer Communication Review*, *34*(1), 51. doi: 10.1145/972374.972384.
17. Roesch, M. (1999). Snort-lightweight intrusion detection for networks. In *Proceedings of the 13th USENIX conference on system administration* (pp. 229–238). Seattle, Washington.
18. Vigna, G. ve Kemmerer, R. A. (1999). NetSTAT: A network-based intrusion detection system. *Journal of Computer Security*, *7*(1), 37–71. doi: 10.3233/jcs-1999-7103.
19. Symantec. (2017, April). Internet security threat report 2017. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf.
20. Ye, N., Emran, S., Chen, Q. ve Vilbert, S. (2002). Multivariate statistical analysis of audit trails for host-based intrusion detection. *IEEE Transactions on Computers*, *51*(7), 810–820. doi: 10.1109/tc.2002.1017701.
21. Kshetri, N. ve Voas, J. (2017). Hacking Power Grids: A Current Problem. *Computer*, *50*(12), 91–95. doi: 10.1109/mc.2017.4451203.
22. Xiao, L., Wan, X., Lu, X., Zhang, Y. ve Wu, D. (2018). IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security? *IEEE Signal Processing Magazine*, *35* (5), 41–49. doi: 10.1109/msp.2018.2825478.
23. Chebrolu, S., Abraham, A. ve Thomas, J. P. (2005). Feature deduction and ensemble design of intrusion detection systems. *Computers & Security*, *24* (4), 295–307. doi: 10.1016/j.cose.2004.09.008.
24. Fu, Y., Sandhu , K. ve Shih, M.-Y. (1999). Clustering of Web Users Based on Access Patterns. In *Proceedings of the 1999 KDD Workshop on Web Mining*.
25. Etzioni, O. (1996). The World-Wide Web: quagmire or gold mine? *Communications of the ACM*, *39*(11), 65–68. doi: 10.1145/240455.240473.
26. Cooley, R., Mobasher, B. ve Srivastava, J. (1997). Web mining: information and pattern discovery on the World Wide Web. In *Proceedings Ninth IEEE International Conference on Tools with Artificial Intelligence*.
27. Joshi, K. P., Joshi, A., Yesha, Y. ve Krishnapuram, R. (1999). Warehousing and mining Web logs. *Proceedings of the Second International Workshop on Web Information and Data Management - WIDM 99*. doi: 10.1145/319759.319792.
28. Srivastava, J., Cooley, R., Deshpande, M. ve Tan, P.-N. (2000). Web usage mining. *ACM SIGKDD Explorations Newsletter*, *1*(2), 12. doi: 10.1145/846183.846188.
29. Zaiane, O., Xin, M. ve Han, J. (n.d.). Discovering Web access patterns and trends by applying OLAP and data mining technology on Web logs. *Proceedings IEEE International Forum on Research and Technology Advances in Digital Libraries -ADL98-*. doi: 10.1109/adl.1998.670376.
30. Portnoy, L. (2000). Intrusion detection with unlabeled data using clustering. Columbia University, Columbia.

Bölüm 3

AÇIK KAYNAK İSTİHBARATI (OPEN SOURCE INTELLIGENCE OSINT)

Hüseyin Akarslan

Kısacası kamuya açık kaynaklardan elde edilebilecek verilen toplanması ve analiz edilmesi süreci olarak tanımlanabilecek açık kaynak istihbaratı (open source intelligence - OSINT) bu çalışmada disiplinler arası bir bakış açısıyla farklı yönleriyle ele alınmıştır. Kapsamı itibariyle çok geniş bir konu olan açık kaynak istihbaratı önemini giderek arttırmaktadır. Birçok farklı alanda başarıyla hayata geçirilen bir yöntem olan açık kaynak istihbaratının temel prensipleri, metodolojisi ve güncel teknolojik gelişmelere nasıl entegre edilebileceği uygulamadan örneklerle açıklanmıştır. Genel bir çerçeve çizilen bu çalışma da ele alınan alt başlıklar daha derinlemesine incelenebilecek konular olduğundan kapsamı genişletmeme adına öz bilgiler ışığında tartışılmıştır. Her bölümde açık kaynak istihbaratı ile ilgili popüler eğilimlere değinilmiş ve son bölümde ise gelecekte yaşanabilecek gelişmeler vurgulanmıştır.

3.1. GİRİŞ

İnsanlık tarihinin bilgi ile olan ilişkisi internet teknolojilerinin yaygınlaşmasıyla son otuz yılda çok ciddi bir değişim yaşamıştır. Çünkü 1990'lı yıllara kadar "bilgiye ulaşmak" en önemli mesele iken günümüzde bu problem ortadan kalkmış ve bunun yerine "ulaşılan bilgiyi değerlendirmek" bir mesele hâline gelmiştir. İstihbarat terimi, gizlilik, sırlar ve erişilmesi mümkün

olmayan mahrem bilgiler gibi kavramları çağrıştırmaktadır. Ancak konunun günümüzdeki ve geçmişteki uzmanları, istihbaratın gizli bilgilerden ziyade açık kaynaklardan erişilebilir veriler üzerine yürütülen bir süreç olduğunu Sn. Hakan FİDAN'ın *yaptığı tez çalışmasında; "Hiçbir analist, kamuya açık kayıtlarda (açık kaynak) ne olduğunu dikkate almadan yalnızca gizli bilgilerle kolaylıkla bir sonuca varamaz." olarak* net bir şekilde ifade edilmiştir.

Devletlerin tarihi kadar eski bir geçmişi olan istihbarat dünyası son yüzyılda ciddi değişiklikler geçirirken en büyük kırılımı 20. yüzyılın sonu ve 21. yüzyılın başlarında gerçekleşmiştir. Modern istihbaratın en önemli bileşeni olan açık kaynak istihbaratı (open source intelligence - OSINT) internet, büyük veri ve yapay zekâ gibi teknolojilerin gelişimi ile çok kısa bir zaman diliminde adeta evrim geçirmiştir. Hızla artan açık veri kaynaklarından erişilebilir verinin toplanması, işlenmesi ve analiz edilerek kıymetlendirilmesi için büyük veri yaklaşımının benimsenmesi ve yapay zekâ algoritmalarının kullanılması artık bir tercihten öte zorunluluk hâlini almıştır. Nitekim bu durumun pratik örnekleri hem kamu hem de özel sektör uygulamalarında günbegün hayata geçirilmektedir.

3.2. AÇIK KAYNAK İSTİHBARATI

İstihbarat kelimesinin anlamına bakıldığında farklı disiplinler açısından farklı tanımları olduğu görülmektedir. Türk Dil Kurumu sözlüğünde istihbarat; "Yeni öğrenilen bilgiler, haberler, duyumlar. Bilgi toplama, haber alma." olarak ifade edilmektedir [1]. Güvenlik Terimleri Sözlüğü'nde ise; "İstihbarat, kullanıcıların talep ve ihtiyaçlarına yönelik olarak, değişik kaynaklardan bilgilerin toplanması ve bu bilgilerin bir dizi işlemden geçirilerek yorumlanması sonucu elde edilen nihaî ürün; kısaca, üretilmiş, genellikle gizli ve daha çok eyleme/aksiyona yönelik olan zamanlı bilgidir." şeklinde tanımlanmıştır [2]. İstihbarat kavramının İngilizce karşılığı olan "intelligence" kelimesi "toplanılan gizli bilgi" olarak tanımlanmaktadır [3].

Tanımlardan da anlaşılacağı üzere, istihbarat ham veri ya da bilgiden öte bir sürecin sonucu olarak ortaya çıkmaktadır. Bilgi değer zinciri olarak ifade

edilen ham veriden organizasyonel sonuçlar elde etme sürecinde, istihbarat belli basamakların çıktısı olduğu gibi belli basamakların da girdisi niteliğindedir.

Şekil 3.1. Bilgi Değer Zinciri [4]

Tarihi geçmişi çok eskilere dayanan istihbarat kavramının 2. Dünya Savaşı'yla birlikte ciddi bir evrim geçirdiği görülmektedir. 20. yüzyılda ulaşılan istihbarat teknolojileri ile gelişen modern istihbarat ve modern öncesi istihbarat arasında ciddi farklılıklar bulunmaktadır.

Tablo 3.1. Modern Öncesi ve Modern İstihbarat Karşılaştırılması [5]

	Modern Öncesi İstihbarat	Modern İstihbarat
Bilgi Kaynağı	□ Tamamen insani istihbarat	□ Açık kaynaklar, □ Bütün yeni istihbarat türleri, □ İnsani istihbarat
Güvenilirlik	□ Güvenilirlik düşük, □ Doğrulama Zor, □ Aldatma için kullanmaya eğilimli	□ Görece yüksek doğrulanabilir, □ Değişik istihbarat kaynakları tarafından desteklenebilir
Elde Edilebilirlik	□ Yavaş, □ Önemli olmak için çok geç, □ Olaylar tarafından aşılıyor	□ Çabuk, □ Gerektiğinde elde edilebilir
İstihbarata Verilen Önem ve Talep	□ Ilımlı talep, □ Önemli görülmekle birlikte yaşamsal değil, □ Genelde istihbaratın kötümser ve negatif değerlendirilmesi	□ Çok yüksek talep, savaş ve barışta, □ Önemli ve yaşamsal, □ İstihbaratın önemli/pozitif değerlendirilmesi,
Örgüt	□ Genellikle geçici, □ Ayrı bir meslek değil, □ Az sayıda üye	□ Büyük ve profesyonel örgüt, □ Sürekli örgüt, □ Kompleks istihbarat toplama
İstihbarat Döngüsü	□ Temel dört aşama; Tespit, toplama, işleme, dağıtım	□ Temel dört aşama; Tespit, toplama, işleme, dağıtım
Analiz	□ Sınırlı enformasyon, □ Yoğun insan gücü	□ Sürekli artan enformasyon ortam bilgisayar desteği

Çalışmamız açısından modern öncesi ve modern istihbaratı karşılaştırdığımızda iki önemli husus dikkat çekmektedir. Bunlardan birincisi artık açık kaynakların ciddi bir bilgi kaynağı hâline gelmesi ikincisi ise büyük miktarda verinin işlenebilip kıymetlendirilebilmesi için bilgisayar teknolojilerine ihtiyaç duyulmasıdır.

3.2.1. Açık Kaynak İstihbaratının Sınıflandırılması

Zaman içinde değişen koşullara göre istihbarat farklı başlıklar altında kategorize edilmektedir. Literatürde değişiklikler olmakla birlikte genel olarak iki farklı kategoride istihbarat türleri sınıflandırılmaktadır. Birincisi istihbaratın alanına göre sınıflandırma, ikincisi ise istihbaratın toplanma şekline göre sınıflandırılmadır [6].

Alanlarına göre;

- siyasi istihbarat,
- askerî istihbarat,
- ekonomik istihbarat,
- sosyal istihbarat,
- coğrafi istihbarat,
- biyografik istihbarat,
- ulaşım ve iletişim istihbaratı,
- bilim ve teknoloji istihbaratı ve
- siber istihbarat

olarak sınıflandırılmaktadır. Toplanma şekline göre ise iki temel kategoriye ayrılmaktadır. Bunlar;

- insan istihbaratı (Human Intelligence-HUMINT) ve
- teknik istihbarat (Technical Intelligence-TECHINT).

Teknik istihbarat bir dizi teknik yöntemin kullanılarak istihbarat toplanmasıdır. Teknik istihbarat başta;

- sinyal istihbaratı (Signal Intelligence-SIGINT) olmak üzere,
- fotoğraf istihbaratı (Imagery Intelligence-IMINT),
- uydu istihbaratı, nükleer istihbarat, radar istihbaratı (Radar Intelligence-RADINT),
- elektronik istihbarat (Electronic Intelligence-ELINT),
- akustik istihbarat, elektromanyetik istihbarat ve tıbbi istihbarat

gibi alt kategorilere ayrılmaktadır [7].

Açık kaynak istihbaratı (Open Source Intelligence-OSINT) ise kamunun erişimine açık her türlü basılı ve elektronik ortamdaki bilgiden elde edilen istihbarat şeklinde tanımlanmaktadır. Bu erişim tamamen herkese açık olduğu gibi gri literatür [8] denilen bazı kısıtlamalarla belirli katılımcı ya da organizasyonların erişimine açık alanı da kapsamaktadır [9]. Gri literatürdeki yayınlar klasik yayımcılık modellerinin dışında üretilmekte ve dağıtılmaktadırlar.

Açık kaynak istihbaratı ile ilgili en önemli açıklamalardan birisi Amerikan Savunma İstihbaratı eski başkanı Korgeneral Samuel V. Wilson'a aittir. 1997

yılında Washington Post gazetesine verdiği bir röportajda "*İstihbaratın yüzde doksanı açık kaynaklardan gelmektedir. Sadece kalan yüzde onu gizli bilgilerdir ama daha dikkat çekicidir. Asıl istihbarat kahramanı Sherlock Holmes'dur, James Bond değil. Çünkü Sherlock Holmes herkese açık olan verilerden anlam çıkarmakta, James Bond ise ona özel sunulan araçları kullanmaktadır…*" ifadelerinde bulunmuştur [10].

Açık kaynak istihbaratını dört farklı kategoride ele almak mümkündür. Bunlar [11];

1. ***Açık Kaynak Veri (Open Source Data-OSD):*** Açık kaynaktan elden edilen ham veri.
2. ***Açık Kaynak Bilgi (Open Source Information-OSI):*** Açık kaynaktan elde edilen anlamlandırılmış veri, bilgidir.
3. ***Açık Kaynak İstihbarat (Open Source Intelligence-OSINT):*** Açık kaynaktan elde edilen doğrudan istihbari değeri olan kıymetli bilgidir.
4. ***Doğrulanmış Açık Kaynak İstihbaratı (OSINT-V):*** Açık kaynaktan elde edilen bilgilerin diğer kaynaklarla birlikte doğrulandığı, yüksek kesinlik derecesine sahip istihbarattır.

İstihbarat kaynaklarının ne kadarının açık kaynak olduğu ve ne kadarının elektronik ortamda olduğu 1990'lı yıllardan itibaren tartışılmış ve normal olarak hiçbir zaman net bir oran tespit edilememiştir. Ancak burada oran ne olursa olsun elde edilen verilerden bütüncül bir değerlendirme yapılabilmesi için hem açık hem de açık olmayan kaynakların birbirinin tamamlayıcısı olarak kabul edilerek analiz yapılması gerektiği düşüncesidir [12].

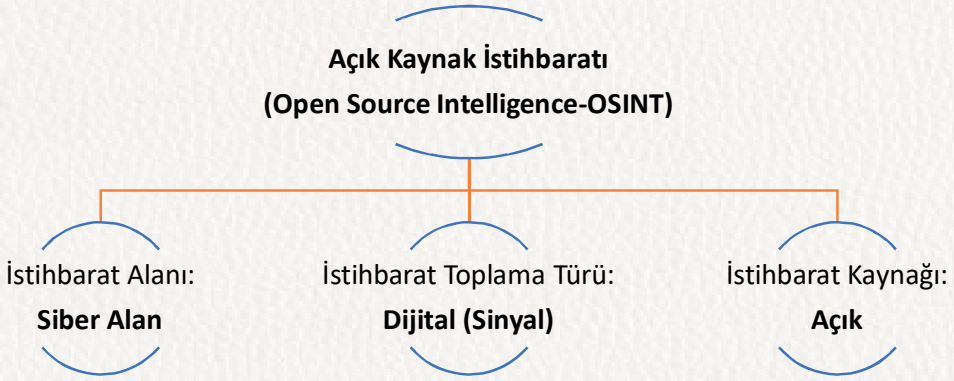
Tarihsel sürece baktığımızda 19. yy., 20. yy. ve 21. yy.'da istihbarat paradigması ciddi bir değişim yaşamıştır. 1844 yılında Baltimore ile Washington arasında ilk telgraf hattının devreye alınmasıyla başlayan elektronik haberleşme, telefonla ses haberleşmesinin ve internetle veri iletiminin yayılmasıyla çok farklı bir seviyeye gelmiştir. Bu bağlamda sinyallerin yakalanmasıyla bilgi edinmeye dayanan sinyal istihbaratı, istihbarat dünyasında devrim niteliğinde yenilikler getirmiştir [13]. Klasik sınıflandırmada açık kaynak istihbaratı (OSINT), sinyal istihbaratının (SIGINT) altında kategorize edilmektedir.

Klasik açık kaynak istihbaratı ve dijital açık kaynak istihbaratı farklı olarak ele alınması gereken konulardır [14]. Ancak her ne kadar açık kaynak istihbaratı, dijital olmayan açık kaynaklardan da elde edilen istihbaratı ifade eden bir kavram olsa da günümüzde çoğunlukla "dijital açık kaynak istihbaratı (Digital OSINT)" yerine kullanılmaktadır.

Bu çalışmada da açık kaynak istihbaratı (OSINT) olarak kullanılan kavram, istihbaratın alanı açısından siber istihbarat, istihbarat toplama türü açısından dijital (sinyal) istihbarat ve kaynak olarak açık kaynaklardan elde edilen istihbaratı ifade etmektedir.

İnternet ve onun en etkili aracı olan dünya çapında ağ (World Wide Web-WWW) insan istihbaratının tüm eksenini ve etki alanını değiştirmekle birlikte hedef odaklı çalışan insan zihninin bilgi evreninin derinliklerine inebilmesini sağlamıştır [15].

İnternet dünyası sayesinde insanlar arasında yeni bir "komşuluk (neighborhood)" kavramı da ortaya çıkmaktadır. Kullanıcıların paylaşımları, ürettikleri içerikleri, yorumları, gezdikleri internet siteleri belli platformlar sayesinde kaydedilmekte ve tasniflenmektedir. Bunun yanında ulusal, bölgesel ve yerel kayıtlar, ceza ve medeni hukuk kayıtları, ikamet ve telefon rehberleri, işveren web siteleri, iş rehberleri, meslek birlikleri ve internetten erişilebilen benzer dosyalar dâhil olmak üzere çevrimiçi olarak ulaşılabilir durumdadır. Artık araştırmacılar kişilerin "mahalli araştırmalarını (neighborhood investigations)" siber alandaki açık kaynaktan da yapmaktadırlar [16].



Şekil 3.2. Günümüzde Açık Kaynak İstihbaratı (Open Source Intelligence-OSINT)

Bilgi güvenliği alanında da açık kaynak istihbaratı (OSINT) sıklıkla kullanılan bir kavramdır. Bilgi güvenliği bağlamında hem atağa dayalı (offensive) hem de savunmaya dayalı (defensive) uygulamaların ilk basamağı olan bilgi toplama (keşif-reconnaissance) sürecinde açık kaynak istihbaratı en önemli enstrümanlardan birisi konumundadır. Özellikle zafiyet analizi işlemleri ve siber saldırı eylemlerinin etkili olabilmesi için ilk adım olan başarılı bir bilgi toplama (keşif) sürecinin açık kaynaklar üzerinden yapılması gerekmektedir [17].

3.2.2. Açık Kaynak İstihbaratının Avantajları ve Dezavantajları

Açık kaynak istihbaratı iki ucu keskin bıçak şeklinde ifade edilmektedir. Açık kaynak istihbaratı üzerine çalışan birimler bu gerçeğin bilincinde olarak istihbarat toplama ve analiz süreçlerini hassasiyetle yürütmek zorundadırlar.

Açık kaynak istihbaratının sağladığı en büyük kolaylık, bilgiye erişmenin diğer istihbarat elde etme yöntemlerine göre çok daha zahmetsiz ve risksiz olmasıdır. İkinci dünya savaşından itibaren açık kaynaklardan istihbarat toplayan personelin diğer alanlardan istihbarat toplayan personele göre daha rahat olduğu tecrübe edilmiştir [18].

Açık kaynak istihbaratının sağladığı ciddi avantajlar olmakla birlikte birtakım zorluklar ve problemleri de beraberinde getirmektedir. İlk göze çarpan durum açık kaynak istihbaratından elde edilen verilerin büyük miktarda olmasıdır. Bu durum avantaj gibi gözükse de bu kadar büyük miktarda veriyi işlemek, analiz etmek ve anlamlandırmak hem istihbarat servisleri hem de özel organizasyonlar tarafından ciddi bir iş yüküdür. Çünkü gri bir alan olarak nitelendirilen açık kaynaklardan elde edilen verilerin hangilerinin analiz süreçlerine dâhil edileceğine karar vermek dahi zor bir süreç olarak kabul edilmektedir [19].

Elde edilmek istenilen spesifik bir bilgiye açık kaynaklar üzerinden erişebilmek çoğu zaman mümkün olmamaktadır. Özellikle karşı istihbarat servislerinin ya da özel şirketlerin gizlilik önlemleri kapsamında bu tarz çok değerli veriler açık kaynaktan erişilebilmekten çıkartılmaktadır. Bu hâliyle açık kaynak istihbaratından elde edilen veriler hayati öneme sahip bilgiler olarak değerlendirilmemektedir [20].

Açık kaynak istihbaratının başka bir önemli avantajı ise toplumsal ekonomik ve siyasi hareketlerin analizinin yapılmasına fırsat tanıyacak kolay erişilebilir

büyük miktarda veri sağlamasıdır. Başka bir insan istihbaratı ve/veya teknik istihbarat kullanılmadan toplumlarla ilgili olarak açık kaynak istihbaratından ciddi veriler toplanabilmektedir. Ancak stratejik bir analiz yapılabilmesi için bu veriler tek başına yeterli olmamaktadır, üstelik demokrasi ve özgürlükler bağlamında görece kapalı toplumların kitlesel değişim gösterdiği dönemlerde açık kaynaklardan elde edilen bilgiler yanıltıcı olabilmektedir [21].

Açık kaynaklardan elde edilen verilerin üçüncü taraflarla ya da iş birliği içinde olunan diğer paydaşlarla paylaşılması daha kolay olduğu gibi sert güvenlik protokollerinden de muaftır. Açık kaynaklardan bilgi toplama sürecinde asıl bilgiyi toplayan organizasyonun kendisini farklı kimlikler altında gizlemesi mümkündür. Medyadaki verileri toplayan, tasnifleyen ve analiz edilmeye hazır hâle getiren medya takip şirketleri bu amaçla kullanılmış ve istihbarat servisleri adına çalışmalar yürütmüşlerdir. Toplanan bu veriler ülkeler arasında paylaşılarak askerî istihbarat süreçlerinde aktif olarak kullanılmıştır [22].

Uzak lokasyonlardaki spesifik konularla ilgili güncel bilgiler hızlı bir şekilde açık kaynak istihbaratı ile elde edilebilmektedir. Resmî dokümanlarda yer almayan ya da güncelliğini yitirmiş bilgiler açık kaynaklardan teyit edilerek daha sağlıklı değerlendirme yapılmasını sağlamaktadır. Açık kaynak istihbaratından elde edilen veriler mevcut resmî dokümanlarla doğrulanabileceği gibi başka devletlere ait ele geçirilen resmî dokümanlar da aynı şekilde açık kaynak istihbaratından elde edilen verilerle doğrulanabilmektedir [23].

Kısaca bilgi çarpıtma olarak tanımlanan "dezenformasyon" açısından açık kaynak istihbaratı çok kırılgan yapıdadır. Toplumsal manipülasyon amacıyla propaganda [24] ve karşı-propaganda aracı olarak aktif bir şekilde kullanılan kitle iletişim araçları üzerinden açık kaynak istihbarat analizi yapmak yanlış sonuçlar verebilmektedir.

3.2.3. 21. Yüzyılda Açık Kaynak İstihbaratı

Bilgi ve İletişim teknolojilerindeki gelişmeler 21. yüzyıla damgasını vurmuş hatta bu yüzyılın adının "bilgi çağı", "teknoloji çağı", "internet çağı" gibi kavramlarla anılmasını sağlamıştır. Şüphesiz ki dünyanın çok farklı bölgelerindeki internet kullanıcı sayılarının günden güne artması ve akıllı telefonların yaygınlaşmasıyla birlikte son kullanıcıya hitap eden kişisel mobil uygulamaların adeta patlama yapması, hem veriye erişim he de veri üretme anlamında tam bir paradigma değişimine yol açmıştır.

Tablo 3.2. Dünya İnternet Kullanım İstatistikleri [25]

Dünya İnternet Kullanıcıları ve Nüfus İstatistikleri						
Bölgeler	**Nüfus (2020 Ort.)**	**Toplam Dünya Nüfusuna Oranı**	**İnternet Kullanıcı Sayısı 31 Aralık 2019**	**İnternet Kullanıcılarının Toplam Nüfusa Oranı**	**Büyüme 2000-2020**	**Toplam İnternet Kullanıcılarına Oranı**
Afrika	**1.340.598.447**	17,2 %	**526.374.930**	39,3 %	11.559 %	11,5 %
Asya	**4.294.516.659**	55,1 %	**2.300.469.859**	53,6 %	1.913 %	50,3 %
Avrupa	**834.995.197**	10,7 %	**727.814.272**	87,2 %	592 %	15,9 %
Latin Amerika / Karayipler	**658.345.826**	8,5 %	**453.702.292**	68,9 %	2.411 %	10,0 %
Orta Doğu	**260.991.690**	3,9 %	**180.498.292**	69,2 %	5.395 %	3,9 %
Kuzey Amerika	**368.869.647**	4,7 %	**348.908.868**	94,6 %	222 %	7,6 %
Okyanusya / Avustralya	**42.690.838**	0,5 %	**28.775.373**	67,4 %	277 %	0,6 %
DÜNYA TOPLAMI	**7.796.615.710**	**100,0 %**	**4.574.150.134**	**58,7 %**	**1.167 %**	**100,0 %**

İstatistikler incelendiğinde son yirmi yılda dünya internet kullanıcılarının sayısı "on bir" kattan daha fazla arttığı görülmektedir. Açık kaynak istihbaratının ana kaynağını oluşturan siber alanın, iletişim katmanı açısından en az "on bir" kat büyüdüğü görülmektedir. Bununla birlikte bu iletişim kanalını kullanan milyarlarca internet kullanıcısının ürettiği içerik de dikkate alındığında açık kaynak istihbaratı açısından son yirmi yıldaki büyümeyi hesaplamak dahi çok ekstra bir çalışma yapmayı gerektirmektedir.

21. yüzyılda kamuya açık ya da açık kaynak olarak ifade edilen verilerin üretilmesi, kaydedilmesi ve paylaşılması açısından tam bir devrim yaşanmıştır. İnternet ve dünya çapında ağın (www) hızlı büyümesinin yanı sıra, mobil iletişim teknolojisinin yaygın olarak benimsenmesi ve ilerlemesi ile birlikte açık kaynak istihbaratının kullanılması, istihbarat, politika ve iş dünyasını doğrudan tesiri altına almıştır. Bu devrim, insanların sosyal ve profesyonel olarak nasıl bilgi edindiklerini, fikirlerini nasıl ifade ettiklerini ve birbirleriyle nasıl etkileştiklerini ciddi ölçüde değiştirmiştir. Önemli bir şekilde, geleneksel bilgi kaynakları ve kanallar bu yeni sanal ortama uyum sağlamak ve doğru bilginin sahibi olarak varlıklarını korumak için büyük çaba sarf etmiş olsa da son kullanıcının yükselişi üretilen içerik, özellikle sosyal medya, bilgi ortamını büyük ölçüde farklılaştırmıştır [26].

Sosyal medya 21. yüzyılda ortaya çıkan en önemli mecralardan birisi olmuştur. Açık kaynak istihbaratının en kritik bileşenlerinden birisi olan sosyal medya ile ilgili ABD Özel Kuvvetler komutanlığı görevini yürüten bir general; "*Hepimiz bu alanı (sosyal medya) rutin bir operasyon alanı olarak görmeliyiz: İnsanların nasıl etkileştiklerini yeniden tanımlıyor. Bu araçları kullanmadaki başarımız, incelediğimiz ağları ne kadar iyi analiz ettiğimize göre belirlenecektir.*" şeklinde açıklamalarda bulunmuştur [27].

Organizasyonların bilgi teknolojisini (BT) kullanma biçimi son yirmi yılda önemli ölçüde değişmiştir. Sosyal medya, bulut bilişim ve bilgi teknolojilerinin son kullanıcı tarafında yoğunlaşması gibi yeni eğilimlerin ortaya çıkması, daha fazla verimlilik, maliyet tasarrufu ve yeni iş fırsatlarının paylaşılması, manipüle edilmesi ve suiistimal edilmesi üzerinde derin etkiler yaratmıştır. Siber güvenlik perspektifinden bakıldığında organizasyonlar ve çalışanları, kötü amaçlar için kullanılabilecek açık kaynaklardan erişilebilir veriler üretmektedir [28].

3.3. AÇIK KAYNAK İSTİHBARATI TOPLAMA SÜRECİ

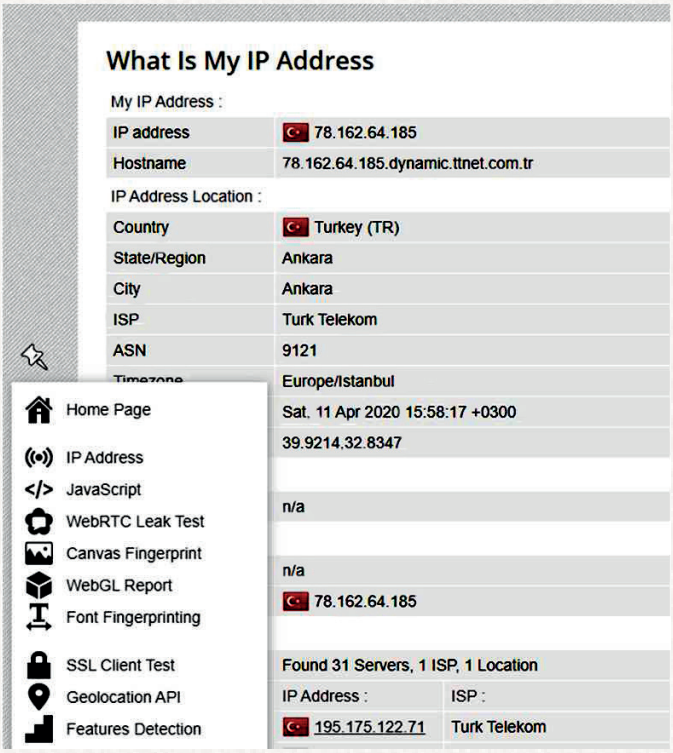
Açık kaynaklardan üç farklı şekilde bilgi toplanmaktadır [29];

- ***Pasif bilgi toplama:*** En güvenli açık kaynak istihbarat toplama yöntemidir, çünkü sadece tamamen kamuya açık kaynaklara erişim sağlanmaktadır. Bu yöntemde anonim kalınması mümkündür çünkü hedef alınan kaynağa erişmek için istemci tarafından hiçbir bilgi (dijital ayak izi) gönderilmemektedir.
- ***Yarı pasif bilgi toplama:*** Pasif bilgi toplama yöntemine göre biraz daha risklidir, çünkü hedef alınan kaynak sisteme erişebilmek için bazı bilgiler istemci tarafından gönderilmek zorundadır. Ancak yine de bağlantı izlerinin belli bir seviyeye kadar gizlenmesi mümkündür. Hedef alınan açık kaynak sistem yöneticileri iyi seviyede teknik bilgiye ve iletişim alt yapısına sahip ise veri toplayan kullanıcıları tespit edebilmektedir.
- ***Aktif bilgi toplama:*** Bu yöntemde hedef alınan açık kaynak sistemi ile istemci karşılıklı olarak tamamen birbirini doğrulamak zorundadır. Bu yöntem bazı senaryolarda erişilen açık kaynak sistemi belirli hedefe yönlendirmek için bilinçli olarak da uygulanmaktadır.

3.3.1. Açık Kaynak İstihbaratı Toplama Öncesi Hazırlık

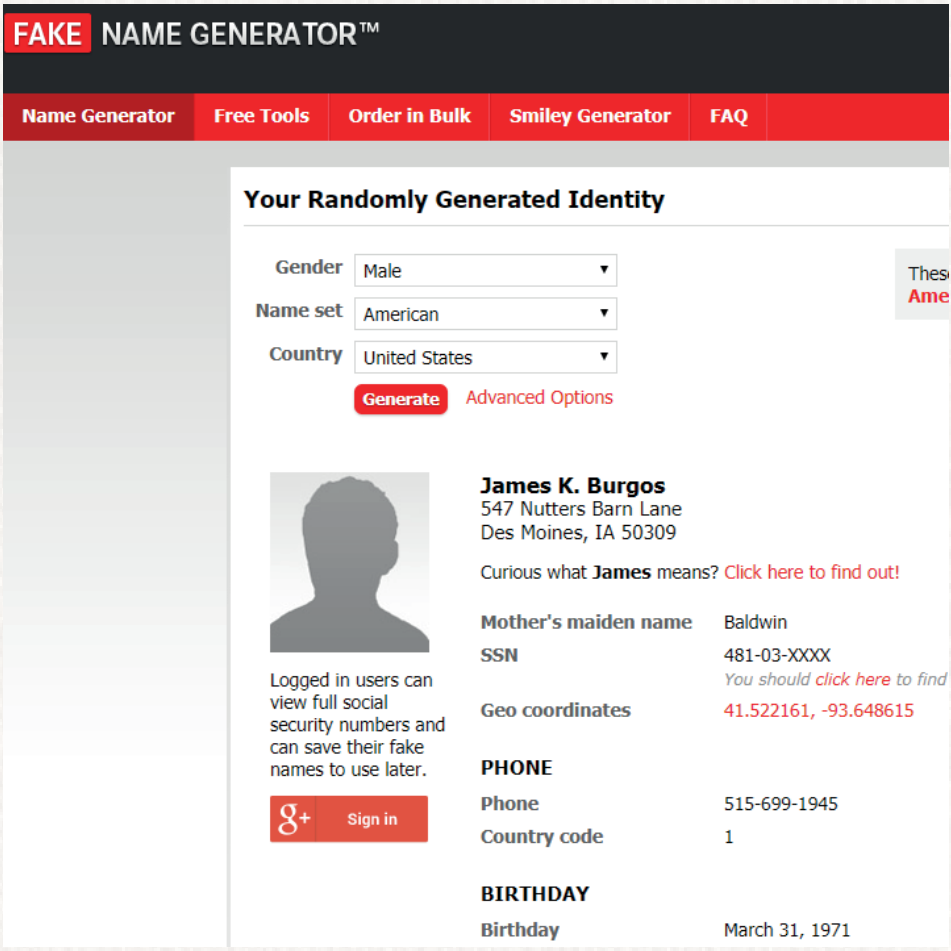
Açık kaynaklardan bilgi toplama işlemine başlamadan önce bilgi güvenliğinin sağlanabilmesi için bazı teknik önlemlerin alınması gerekmektedir. Internet üzerinden iletişim kurulurken erişilen hedef sisteme gerçek IP adresi bilgisinin gönderilmemesi için basit önlemler yeterli olmaktadır. Sanal sunucu, VPN ya da Vekil Sunucu (Proxy) gibi teknolojilerin kullanılması IP adresinin gizlenmesi için çoğu senaryoda etkili bir çözüm olarak kabul edilmektedir.

Web sitelerine erişim esnasında hangi bilgilerin karşı tarafa gönderildiği ile ilgili basit web uygulamaları da kullanılabilmektedir. Bunlara örnek olabilecek bir uygulama "*www.browserleaks.com*" adresi üzerinden hizmet vermektedir. Bu site üzerinden IP adresi, javascript seçenekleri, coğrafi lokasyon gibi erişilen sistemlere dijital ayak izlerin bırakılabildiği birçok özellik kontrol edilebilmektedir.



Şekil 3.3. "www.browserleaks.com" Web Sitesi Ekran Çıktısı

Web sitelerine bağlanılırken işletim sistemi ve internet gezgini tarafından otomatik olarak üretilen çerezler ve geçici dosyalar açık kaynak araştırması öncesinde temizlenmelidir. Giriş yapılmış hesap bilgileri silinmeli ve eğer internet tarayıcısı uygulama (Chrome, Firefox) destekliyorsa gizli mod seçeneği (incognito mode) kullanılmalıdır.



Şekil 3.4. "www.fakenamegenerator.com" Web Sitesi Ekran Görüntüsü

Aktif bilgi toplama süreçlerinde belli bir açık kaynak sistemine erişebilmek için profil oluşturulması gerekiyorsa, tutarlı bir sahte profil oluşturulmalıdır. Sahte bir sosyal medya hesabı kullanılması gereken durumlarda hiçbir arkadaş bağ-

lantısı olmayan ya da hiçbir detaylı bilgi içermeyen boş bir profil dikkat çekeceğinden açık kaynak araştırmasını sekteye uğratabilecektir. Bu tarz sahte profil üretme işlemine çorap kuklası (sock puppet) denilmektedir [30]. Tutarlı sahte profil üretilebilmek için kullanılabilecek uygulamalardan birisi *"www.fakenamegenerator.com"* web sitesidir. Uygulama üzerinden belli bir bölgede yaşayan, gerçekçi iletişim bilgilerine ve isime sahip bir profil oluşturulabilmektedir.

Açık kaynak istihbaratı toplama sürecine başlamadan önce kullanılacak yazılımlar ve güvenlik programları en son sürümlerine yükseltilmelidir. Ayrıca erişilecek kaynakların güncelliği ve güvenilirliği periyodik olarak kontrol edilmelidir. Araştırılacak web adresleri, e-posta adresleri, sosyal medya hesapları, IP Adresleri ve anahtar kelimeler gözden geçirilmelidir. Açık kaynak istihbaratında büyük miktarda veri toplanması ve işlenmesi süreci ciddi bir donanım kaynağı gerektireceğinden işlemlere başlamadan önce mevcut alt yapı ve yazılım kabiliyetleri gereken seviyeye getirilmelidir.

Son olarak açık kaynak istihbaratı toplama işlemi eğer bir organizasyon tarafından yapılıyorsa organizasyonun yazılı ve yazılı olmayan kuralları gözden geçirilerek herhangi bir kuralın ihlal edilmesi önlenmelidir. Aynı şekilde erişilecek açık kaynak platformunun da şartları ve kuralları incelenerek mevcut haklar çerçevesinde süreç yönetilmelidir.

3.3.2. Açık Kaynak İstihbaratı Döngüsü

Klasik istihbarat toplama döngüsü beş temel safhadan oluşmaktadır. İlk aşamada istihbarat toplama sürecinde neyin nasıl yapılacağı ile ilgili bir **planlama** yapılmaktadır. İkinci aşamada belirlenen plan doğrultusunda **bilgi toplanmaktadır**. Toplanan bilgiler **işlenerek** bir istihbarat raporu oluşturulmaktadır. Toplanan ve raporlanan tüm bilgiler tekrardan detaylı olarak **analiz** edilerek neyin, nasıl, neden olduğu ve gelecekte ne olacağı sorularının cevabı verilmektedir. Son aşamada elde edilen tüm çıktılar karar vericilere ve ilgililerine **dağıtılmaktadır** [31].

Açık kaynak istihbarat döngüsü ile ilgili farklı modeller geliştirilmekle beraber ana hatlarıyla klasik istihbarat toplama döngüsüne bire bir benzemektedir;

1. ***Planlama Aşaması (Planning):*** Bu aşamada açık kaynaklardan toplanacak bilgiler tespit edilmektedir. Gereksinimlere göre takip edilecek adımlar öncelik sırasına göre belirlendikten sonra bilgi toplama işleminin sonunda ulaşılması gereken hedefler netleştirilir.

2. ***Bilgi Toplama Aşaması (Collection):*** Erişilmesi planlanan açık kaynaklara erişilerek her türden verilerin toplanması ve muhafaza edilmesi sürecidir. Bilgi toplama farklı kaynaklardan, farklı platformlardan ve farklı formatlarda olabilmektedir. Bu aşamada hazır uygulamalar kullanılabileceği, ihtiyaç duyulan durumlarda özel yazılımlar da geliştirmek gerekmektedir.
3. ***Bilgi İşleme Aşaması (Processing):*** Toplanan verilerin analiz işleminde kullanabilmesi için gerekli düzenleme, tasnifleme, doğrulama ve temizleme işlemidir. Açık kaynak istihbaratında büyük miktarda veri toplandığı için bu aşama toplanan verilerin kıymetlendirilebilmesi için çok önem arz etmektedir. Yabancı dilde toplanan veriler analistlerin kendi dilinde analiz yapabilmesi için bu aşamada çeviriye tabi tutulmaktadırlar.
4. ***Analiz Aşaması (Analysis)***: Bilgi işleme aşamasından sonra yapılan analiz işleminin ilk adımı hedeflenen istihbarat açısından faydası olacak ve faydası olmayacak verilerin ayrıştırılmasıdır. Faydalı olabilecek veriler tespit edildikten sonra bu veriler de üç alt aşamada analiz edilmektedirler. Birincisi tespit edilen veriler doğrulanmakta (authentication) yani doğru olanlar ile sahte/yanlış olanlar ayrıştırılmaktadır. İkincisi bütünlük (integrity) açısından verilerin güvenilirliği kontrol edilmektedir. Üçüncü aşama ise toplanan verilerin elde bulunan diğer verilerle birleştirilerek (context) kıymetlendirilmesidir.
5. ***Raporlama Aşaması (Production)***: Bu aşamada artık elde edilen veriler analiz süreçlerinden geçirilerek, kıymetlendirilmiş yani istihbarat hâline gelmiştir. Elde edilen açık kaynak istihbaratı yazılı raporlar, sözlü brifingler, veri görselleştirme araçları ile hazırlanmış diyagramlar ve benzeri materyaller ile bir ürün hâline getirilmekte ve arşivlenmektedir. Açık kaynak istihbaratının dokümantasyonu her aşamada yapılabilmekle birlikte bu aşamada nihai ve en önemli hâlini almaktadır.
6. ***Dağıtım Aşaması (Dissemination)***: Son olarak elde edilen açık kaynak istihbaratı karar vericiler, yöneticiler ya da ilgilileri ile paylaşılmaktadırlar. Açık kaynak istihbaratının dağıtımı ilk olarak süreci başlatan kişi ya da makamla yapılmaktadır.

Açık kaynak istihbaratı toplama süreci bir döngü olduğundan son aşamaya gelindikten sonra tekrar başa dönülmektedir. Dinamik yapısı gereği açık kaynaktan erişilebilen veriler günlük ve hatta anlık değişebileceğinden istihbarat ihtiyacı devam ettiği ve gereksinimler değişmediği sürece bu döngü ara verilmeden devem ettirilmektedir.

Şekil 3.5. Açık Kaynak İstihbaratı Döngüsü

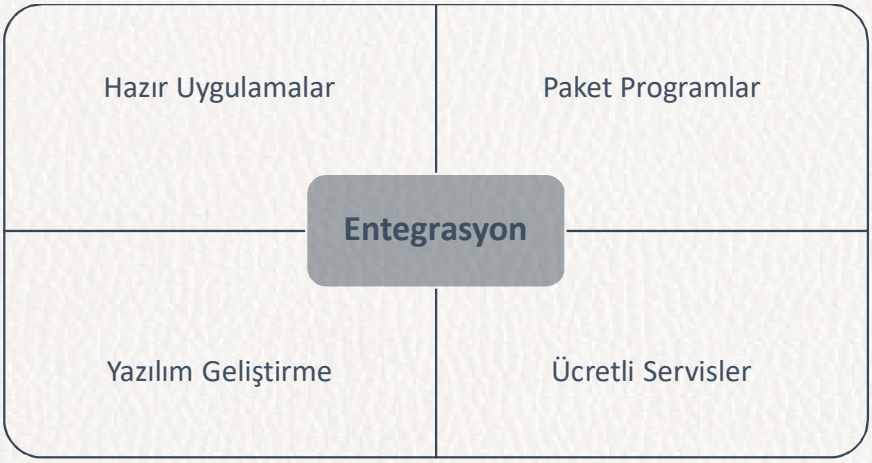
3.3.3. Açık Kaynak İstihbaratı Araçları ve Teknikleri

Açık kaynak istihbaratı döngüsündeki farklı aşamalar için birçok farklı araçlar kullanılabilmektedir. Bu araçların bir kısmı yine doğrudan açık kaynaklardan erişilebilen hazır web/masaüstü uygulamaları şeklinde iken bir kısmı ücretli paket programlar olmaktadır. Bazı durumlarda planlama aşamasında belirlenen açık kaynak istihbaratı toplama hedeflerinin tamamı sadece ücretsiz erişilebilen web uygulamaları ile gerçekleştirilebilirken daha spesifik hedefler için özel geliştirilmiş ücretli paket programlara ihtiyaç duyulmaktadır. Daha

ileri seviye ve kapsamlı açık kaynak istihbaratı süreçlerinde ise organizasyonun öz kaynaklarıyla sadece belli bir işleme yönelik yazılımlar geliştirmesi gerekebilmektedir.

Ücretsiz olarak kullanılan açık kaynak istihbaratı araçlarının bir kısmı açık kaynak lisansı (Open-Source license) ile lisanslandığından, kaynak kodları ihtiyaca göre değiştirilerek kullanılabilmektedir [32].

Bazı firmalar tarafından açık kaynak istihbaratı için kullanılabilecek araçlar hizmet ve danışmanlık servisleriyle birlikte organizasyonlara sunulmaktadır. Bu tür araçlar genel olarak teknik bilgisi yüksek olmayan son kullanıcılar için geliştirilmektedirler böylece kullanıcılar teknik detaylarla uğraşmak yerine asıl görevleri olan veriye odaklanabilmektedirler [33].



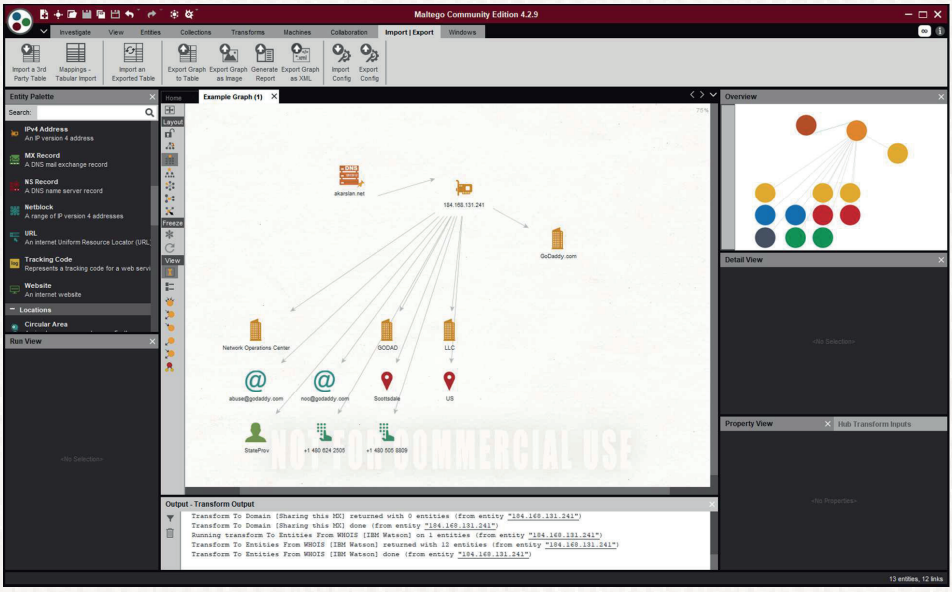
Şekil 3.6. Açık Kaynak İstihbaratı Araçları

Profesyonel bir istihbarat servisi tarafından kapsamlı bir açık kaynak istihbaratı süreci işletilebilmesi için hazır uygulamalar, paket programlar, yazılım geliştirme ve dış servislerin tamamının başarılı bir entegrasyon içinde yönetilmesine ihtiyaç duyulmaktadır.

Hazır açık kaynak istihbaratı uygulamalarının bir kısmı *"www.osintframework.com"* (OSINT Framework) ve *"www.osint.link"* (Open Source Intelligence OSINT Tools & Resources) gibi internet sitelerinde liste hâlinde yayınlanmasının yanı sıra, "Kali Linux" [34] ve "Buscador Investigative

Operating System" [35] gibi bilgi güvenliği temalı geliştirilen linux işletim sistemlerinin içinde düzenlenmiş şekilde gelmektedir.

Açık kaynak istihbaratı için kullanılabilecek etkili araçlardan birisi olan Maltego [36] hem veri toplama hem de gelişmiş veri görselleştirme özellikleri ile diğerlerinden ayrılmaktadır. Maltego, yalnızca verileri ayıklamakla kalmayıp, aynı zamanda verilerin anlaşılması ve analizi kolay bir formatta gösterilebilmesi için platform sağlayan bir OSINT uygulamasıdır [37].



Şekil 3.7. Maltego Programı Ekran Görüntüsü

3.3.3.1. Metin Madenciliği (Text Mining)

En basit tanımıyla mevcut verilerin analiz edilerek normal şartlarda görünmeyen anlamlı bilgilerin ve veriler arasındaki ilişkilerin çıkarılmasına sürecine veri madenciliği denilmektedir. Metin madenciliği ise kaynağının metin verileri olduğu veri madenciliği sürecini ifade etmektedir. Açık kaynak istihbaratı açısından başta sosyal medya platformları olmak üzere erişilebilen verilerin ciddi bir kısmını metinler oluşturduğundan metin madenciliği teknikleri en çok başvurulan açık kaynak istihbaratı tekniklerinin başında gelmektedir.

Metin Madenciliği metin üzerinden yapısallaştırılmış veri elde etmeyi amaçlar. Metinlerin sınıflandırılması, kümelenmesi, metinlerden konu çıkarılması, sınıf taneciklerinin üretilmesi (production of granular taxonomy), duygu analizi (sentimental analysis), metin özetleme ve varlık ilişki modellemesi (entity relationship modelling) gibi çalışmaları hedefler. Bu hedeflere ulaşılması için metin madenciliği çalışmaları kapsamında; bilgi çıkarımı/getirimi (information retrieval), sözcük analizi (lexical analysis), kelime frekans dağılımı, örüntü tanıma (pattern recognition), etiketleme (tagging), bilgi çıkarımı (information extraction) ve görselleştirme (visualization) gibi yöntemler kullanılmaktadır [38].

Metin madenciliğinin kökenleri 50 yılı aşkındır üzerinde araştırmalar yapılan bilgi erişimi (information retrieval) ve doğal dil işleme (Natural Language Processing - NLP) uygulamalarına dayanmaktadır. Internet kullanımının artmasıyla birlikte iletişimde yaşanan dijitalleşme (e-postalar, sosyal medya, internet siteleri vb.) metin içerikli verinin ivmelenerek büyümesine neden olmuştur. Yapılandırılmış ve yapılandırılmamış formatta sürekli biçimde üretilen veriler üzerinde, bilgi erişimi ve doğal dil işlemenin yanı sıra, bilgi çıkarımı, kategorizasyon, ilişkilendirme (association) ve sınıflandırma süreçleri işletilerek tematik yapıların keşfi, tanımlanması, indirgenmesi, anlamlandırılması ve karar süreçlerinde yararlanılması mümkün hâle getirilmiştir [39].

Kullanılan ifadelerde belli kelimelerin tercih edilme oranına dayanan "anahtar kelime analizi (keyness analysis)" ile kişisel özellikler tespit edilebilmektedir [40]. Örneğin İngilizce bir ifadede kullanılan kelimelerin tercih edilme oranına göre kişinin ana dilinin mi İngilizce olduğu yoksa sonradan mı İngilizce öğrendiği veri setine bağlı olarak yüksek oranda tahmin edilebilmektedir [41]. Aynı şekilde "sıklık analizi (frequency profiling)" ile kullanılan ifadedeki kelimelerin sıklığına göre ifadeyi kullanan kişinin farklı dönemleri açısından tespitler yapılabilmektedir. Alzheimer gibi kişinin konuşmasını etkileyen hastalıklarda açık kaynaklardan elde edilen metinlerle kişinin ifadelerini hastalığından önce mi yoksa sonra mı kullandığı tespit edilebilmektedir [42].

Duygu analizi metin madenciliği ile bir konu hakkında kişilerin olumlu, olumsuz ya da nötr gibi duygularının tespit edildiği yöntemdir. Birçok internet kullanıcısı günlük olarak ziyaret ettikleri web sitelerinde ve sosyal

medya platformlarında fikirlerini, görüşlerini ve duygularını yansıtan ifadeler kullanmaktadırlar. Açık kaynaklardan erişilebilen birçok platformda ziyaretçilerin ürün ya da dijital içeriklere yönelik yorumlarından hareketle duyguları analiz edilebilmekte [43] hatta terör örgütü üyelerinin açık kaynaklara yansıyan demeçlerinden aralarındaki duygusal durum benzerliği tespit edilebilmektedir [44].

3.3.3.2. Sosyal Ağ Analizi (Social Network Analysis)

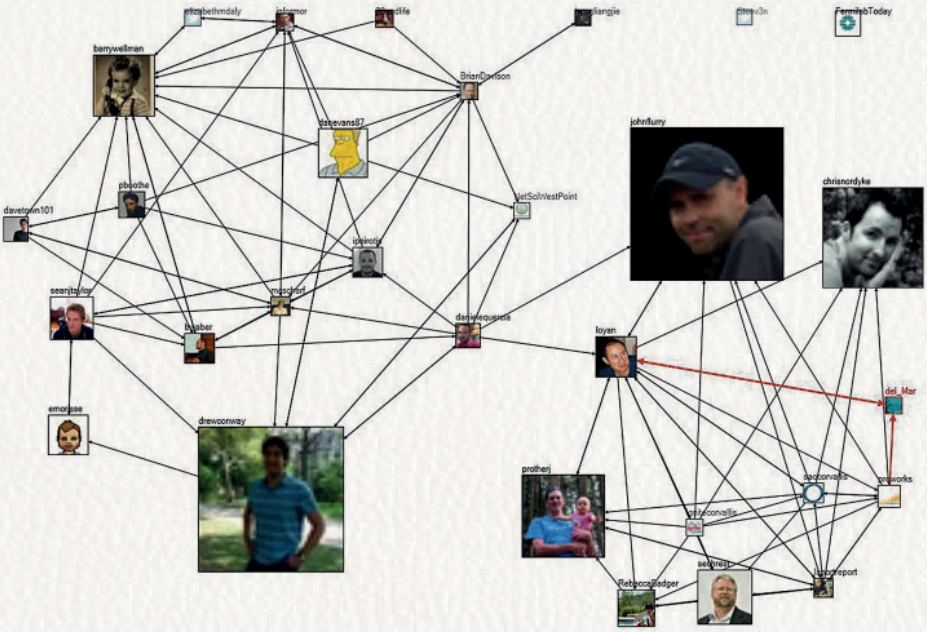
Açık kaynaklarda içerik üreten ya da bu kaynaklarla etkileşim içinde bulunan kullanıcılar bireysel bir eylem gerçekleştirmelerine rağmen aslında büyük bir sosyal ağın parçası durumundadırlar. Bu sosyal ağın gerçek hayatta da bir karşılığı olabileceği gibi (okul arkadaşlarının aynı sosyal medya gruplarına üye olması gibi) tamamen sanal bir ilişki (dünyanın iki farklı ucundaki akademisyenlerin aynı makaleyi okuması gibi) de olabilmektedir.

Sosyal ağ analizi arkadaşlık gibi iki kişi arasındaki yapısal ilişkiyi tespit etmek ve ölçmek için kullanıldığı gibi belli bir fikir etrafında toplanan birden fazla kişi arasındaki ilişkiyi de konu almaktadır. Sosyal ağ analizi bireylerin yanında organizasyonların ya da grupların da aralarındaki ilişkiye dayanarak da yapılabilmektedir [45].

Açık kaynak istihbaratı açısından kullanıcıların birbirinden farklı sosyal medya platformlarındaki etkileşimleri kişiler arasındaki sosyal ağın tespit edilmesi için imkân sağlamaktadır. Farklı platformlardaki açık ilişkilerin dışında gizli arkadaşlıklar, üçüncü kişilerin erişimine kapalı bağlantılar da farklı tekniklerle analiz edilerek açık ve gizli ilişkilerden örülü büyük sosyal ağın yapısı çıkartılabilmektedir [46].

Sosyal ağ analizi gittikçe birbiriyle iletişim içinde olan yeni dünya düzenini anlamak için en ideal araçlardan birisi durumundadır. Sosyal medya etkileşimlerine göre sosyal ağ analizi yapılabilmesi için tasarlanmış araçlar [47] mevcuttur. Sosyal medya, şeffaf yönetim, afetlere müdahale, vatandaşlık hakları ve eğitim eşitliği gibi sosyal gereksinimlerini geliştirecek bir mecra olarak görülmektedir. Ancak son yıllarda siyasi propaganda, dezenformasyon, seçimlerde kitleleri yönlendirme ve aşı karşıtı propagandalar gibi toplum yararı yerine belli grupların amaçlarına hizmet eden bir yapıya dönüşmüştür. Bu dinamik değişimi daha iyi anlamak için sosyal ağ analizi yapan araştırmacılar

açık kaynaklardan elde edilen verilerle daha sağlıklı analiz yapılabilmesi için belli standartlar ve metrikler geliştirmişlerdir. Özellikle yeni sosyal ağ görselleştirme teknikleri ile eğilimler, kümelenmeler, karmaşık ilişki ağları ve farklı kişi veya gruplar arasındaki etkileşim kanalları daha anlaşılır bir biçimde görüntülenebilmektedir [48].



Şekil 3.8. Açık Kaynak İstihbaratına Dayalı Sosyal Ağ Analizi Diyagramı [49]

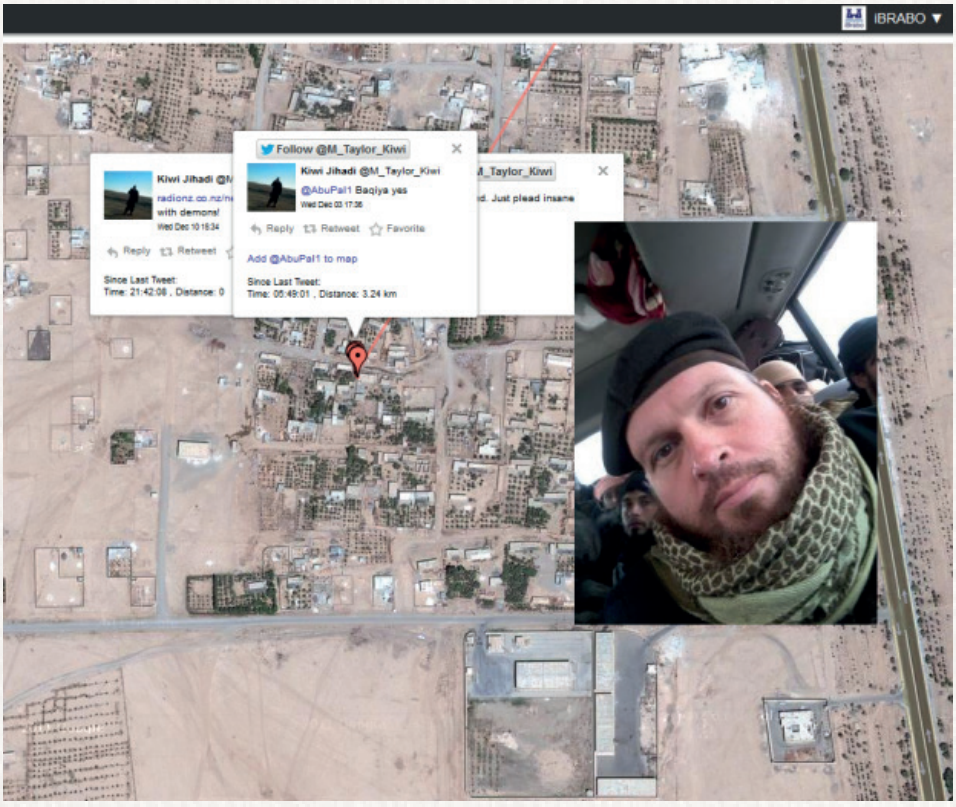
Şekil 3.8'deki örnekte 2009 yılında New York Üniversitesi'nde düzenlenen Ağ Bilimleri Konferansı'ndaki katılımcıların Twitter üzerinden "#WIN09" etiketi ile attıkları tweetlerden kaynaklı ilişki diyagramları çizilmiştir. Atılan tweet sayısına göre profil resimlerinin büyüklükleri değişmekte ve böylece etkin olan aktör ön plana çıkarılmaktadır.

Sosyometri araştırmaları yani bireyin içinde bulunduğu gruptaki diğer kişilerle olan yakınlık ya da uzaklık durumlarının sayısal olarak belirlenmesi ve bunun görsel olarak aktarılması (sosyogram) işlemleri bireylerle bire bir görüşmeyi ve samimi fikirlerini almayı gerektirmektedir. Ancak açık kaynak istihbaratı sayesinde kişilerin sosyal medya paylaşımları ve diğer kişilerle

olan etkileşimleri analiz edilerek normal şartlarda erişilemeyecek kişi ya da grupların sosyal ağ yapıları tespit edilerek gerçek sosyal durumlarına benzer şekilde görselleştirilebilmektedir [50].

3.3.3.3. Mekânsal Analiz (Geospatial Analysis)

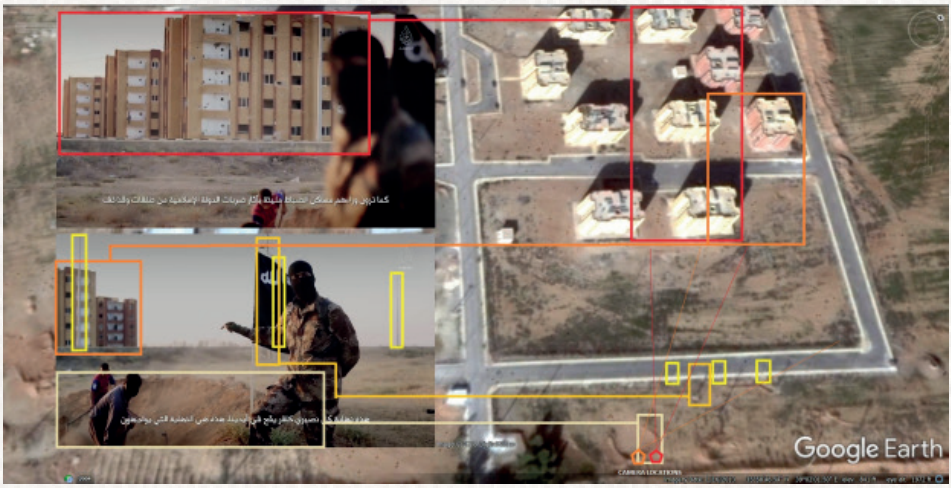
Açık kaynak istihbaratından elde edilen veriler ciddi miktarda coğrafi bilgi içermektedirler. Internet kullanıcıları sosyal medya ve web siteleri üzerinden yaptıkları işlemlerinde bazen bilerek bazen bilmeyerek coğrafi ayak izleri bırakmaktadırlar. Coğrafi etiketleme (geotagging) işlemi ile kullanıcılar sosyal medya paylaşımlarında ve fotoğraf dosyalarında enlem ve boylam bilgilerini akıllı cihazlarındaki GPS çipleri sayesinde tespit ederek eklemektedirler.



Şekil 3.9. Açık Kaynak İstihbaratına Dayalı Konum Bilgisi Tespiti [51]

Konum bilgisi, kişisel verilerden [52] olup üçüncü kişilerle paylaşılmayan verilerdendir ve eğer paylaşılması ve işlenmesi gerekiyorsa ulusal mevzuata uygun bir şekilde hareket edilmesi zorunluluğu vardır. Bu kadar hassas bir veriyi her gün milyarlarca internet kullanıcısı kendi rızasıyla açık kaynaklarda paylaşmaktadırlar. Bu durum açık kaynak istihbaratı analistleri için bulunmaz fırsatlar yaratmaktadır. Konumunu gizli tutmak isteyen suçlular dahi sosyal medya paylaşımlarında bu hataya düşebilmektedirler. Yeni Zelandalı bir yabancı terörist savaşçı DAEŞ Terör Örgütü'ne katılmak için gittiği Suriye'de attığı tweetlerden örgütün gizli yerleşim yerlerini ifşa etmiştir [53].

Açık kaynak istihbarat araçlarında coğrafi-çit (geo-fencing) uygulaması ile belli bir coğrafi sınır içindeki paylaşımlar ve içerikler analiz edilmektedir [54]. Yer tespiti (geolocating) tekniğinde ise özellikle paylaşılan resimlerdeki heykeller gibi belirleyici objeler ve bilindik tarihî mekanlardan hareketle yer tespiti yapılmaktadır. Ayrıca paylaşılan video görüntüleri ile açık kaynaklardan kullanıma sunulan uydu görüntüleri karşılaştırılarak videonun çekildiği yerler tespit edilebilmektedir. Şekil 3.10'daki örnekte DAEŞ Terör Örgütü üyeleri tarafından çekilen ve sosyal medyada paylaşılan videodaki görüntüler ile teröristlerin bulunması muhtemel yerlere ait uydu görüntüleri karşılaştırılarak yer tespiti yapılabilmiştir.



Şekil 3.10. Açık Kaynak Uydu Görüntüleri ile Video Görüntüleri Üzerinden Yer Tespiti [55]

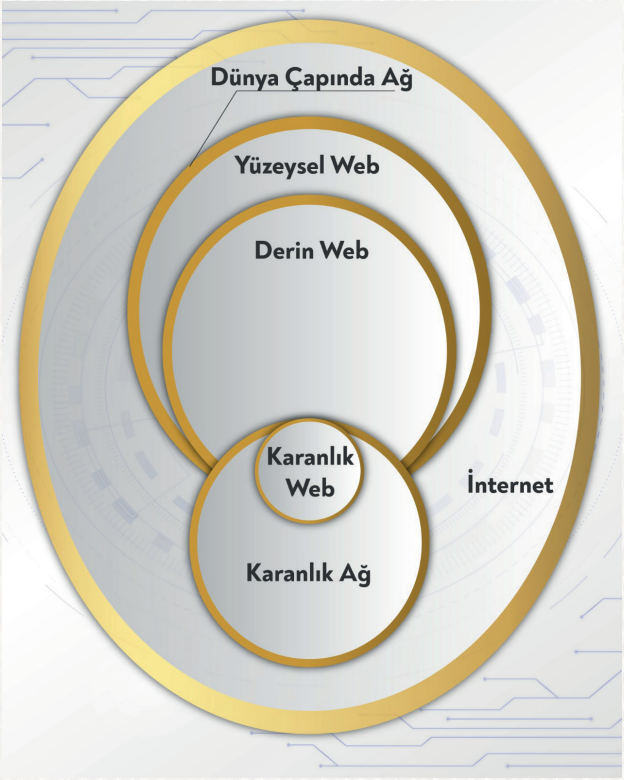
Açık kaynak istihbaratından çok farklı formatta ve çeşitte veri elde edilebildiğinden başarılı bir analiz yapılabilmesi için birçok farklı tekniğin birlikte kullanılması gerekmektedir. Metin verileri, görsel veriler, zaman verileri, coğrafi veriler, ağ trafiği verileri gibi farklı verilerin birlikte analiz edilmesi ile etkili çıkarımlar yapılabilmektedir. Örneğin belli bir tarih ve saatteki bir fotoğraftaki objenin gölge boyuna göre güneş açıları [56] hesaplanarak fotoğrafın muhtemel çekildiği yer tahmin edilebilmektedir.

3.4. DERİN WEB VE KARANLIK WEB AÇISINDAN AÇIK KAYNAK İSTİHBARATI

21. yüzyılda açık kaynak istihbaratının neredeyse tamamını oluşturduğu kabul edilen internet ekosistemi farklı amaçlar ve ihtiyaçlar doğrultusunda değişen yapısıyla üç farklı katmandan oluşmaktadır. İnternetin değişen yapısı açık kaynak istihbaratının da her üç katmana yönelik ilgisinin değişmesini gerektirmiştir. Yüzeysel web (surface web), derin web (deep web) ve karanlık web (dark web) günümüzde internetin üç farklı katmanını oluşturmaktadır [57];

1. ***Yüzeysel Web (Surface Web):*** Arama motorları tarafından indekslenebilen ve standart kullanıcıların internet tarayıcıları ile basit aramalarla erişebildikleri alandır. Bu alanda gündelik ve hassas olamayan verilerin barındırıldığı kabul edilmektedir.
2. ***Derin Web (Deep Web):*** Arama motorları tarafından indekslenemeyen web sitelerinin oluşturduğu alandır. Burada oluşturulan web siteleri spesifik olarak arama motorlarını engellemek yerine, arama motorlarının çalışma prensibine uygun olmayan standart dışı içerikleri nedeniyle indekslenememektedirler. Yüzeysel webdeki içerikler hızla derin web tarafına geçtiğinden açık kaynak araştırmalarını standart arama motorları üzerinden yapmak yetersiz olmaktadır.
3. ***Karanlık Web (Dark Web):*** Karanlık web, yüzeysel web ve derin web ile karşılaştırıldığında ağ yapısı olarak da ayrılan alandır. Karanlık web siteleri Tor [58], FreeNet [59] ve I2P [60] gibi **karanlık ağ (dark net)** denilen farklı platformlar üzerinden hizmet vermektedir. Klasik internet protokolleri ve internet tarayıcıları ile bu alana erişmek mümkün olmamaktadır. Yer altı suç dünyasıyla ilgili en çok kullanılan alan burası kabul edilmektedir.

Avrupa Polis Teşkilatı (Europol) tarafından her yıl yayınlanan İnternet ve Organize Suçlar Risk Değerlendirme Raporu'na göre karanlık web, suçluların suç eşyası alıp sattıkları en önemli ticaret mecrası olarak kabul edilmektedir. Buradaki trafiğin şifreli olması ve en yüksek seviyede anonimliğin sağlanması sebebiyle profesyonel suçlular ile sıradan alıcıların buluşma noktası hâline geldiği tespit edilmiştir. İnternet dünyasındaki kriminal aktiviteler hâlen yüzeysel web ve derin webde de devam etmekle birlikte karanlık web tarafına ciddi bir kaymanın olduğu gözlemlenmektedir [61].

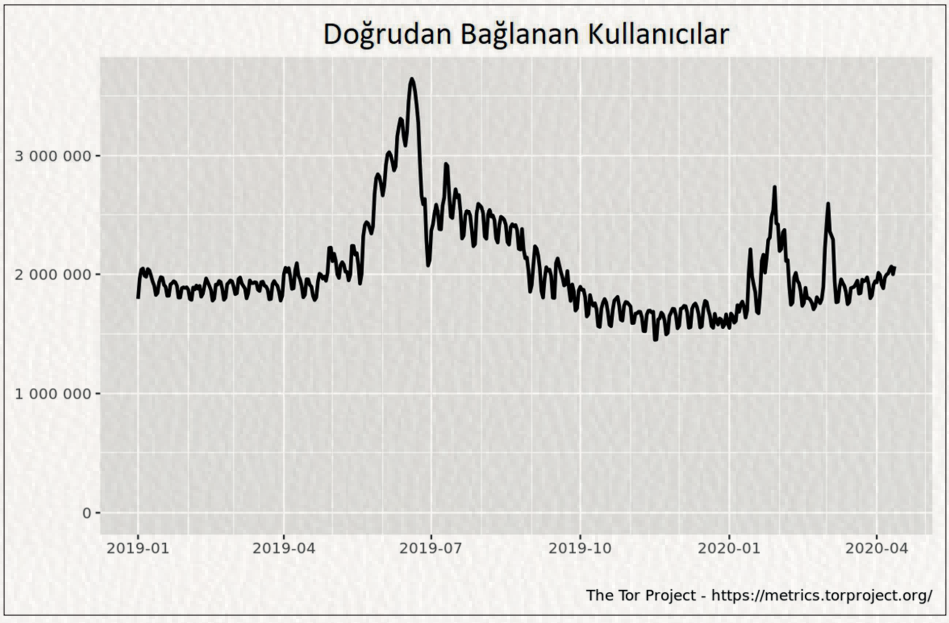


Şekil 3.11. Yüzeysel Web, Derin Web ve Karanlık Web Alt Yapıları

Avrupa Polis Teşkilatı (Europol) tarafından her yıl yayınlanan diğer bir önemli rapor olan AB Terörizm Durum ve Eğilim Raporu'na göre hem yüzeysel web hem de karanlık web siteleri terörizmin finansmanında özellikle kripto paralar üzerinden fon toplamak için yoğun olarak kullanılmaktadır [62].

Karanlık web sitelerinin tamamının kriminal aktiviteler için kullanıldığını söylemek de mümkün olmamaktadır. Özellikle anonimliği [63] ve internette mahremiyeti savunan birçok aktiviste göre yüzeysel webi kullanmak buradaki tüm işlemlerin büyük araştırma şirketleri tarafından toplanarak analiz edildiği gerekçesiyle bilgi güvenliği açısından sakıncalı olarak görülmektedir [64]. Bu yüzden sıradan internet kullanıcıları da hızla karanlık ağ kullanıcısı hâline dönüşmektedir.

Günümüzde ortalama günde 2 milyondan fazla kullanıcının bağlandığı TOR (The Onion Router) ağı en büyük karanlık ağ alt yapısını ".onion" uzantıya sahip Tor sayfaları ise en büyük karanlık web alanını teşkil etmektedir. Açık kaynak istihbaratı açısından bu ciddi kayma önemle takip edilmek ve buna yönelik teknikler geliştirmek zorunluluğu ortaya çıkarmıştır.



Şekil 3.12. 1 Ocak 2019 – 14 Nisan 2020 Tarihler Arası TOR Ağı Günlük Kullanıcı Sayıları [65]

Tam olarak tespit edilmesi mümkün olmamakla birlikte bu alanda yapılan akademik ve teknik çalışmalar incelendiğinde, günümüzde veri boyutu (içerik) açısından karşılaştırıldığında yüzeysel web %4, derin web %95 ve karan-

lık web %1'lik bir oranı oluşturmaktadır [66, 67, 68]. Açık kaynak istihbaratı açısından bakıldığında sadece internet veri havuzunun %4'lük bir kısmını ifade ettiği kabul edilen yüzeysel webe yönelik açık kaynak veri araştırması yapmak büyük resmi kaçırmak anlamına gelmektedir.

Şekil 3.13. Yüzeysel Web, Derin Web ve Karanlık Web Hacimleri

3.5. BÜYÜK VERİ VE AÇIK KAYNAK İSTİHBARATI

Büyük veri (big data) kavramı; verilerin saklanmasında, analiz edilmesinde ve yönetilmesinde klasik veri tabanı yönetim sistemlerin yetersiz kaldığı [69] büyük miktardaki ve sürekli artan verileri ifade etmektedir. Büyük veri kavramının ilk ortaya çıktığı dönemlerde temel karakteristik özellikleri 3V ile tanımlanırken değişen teknolojik yaklaşımlar ve gelişmeler sonucunda günümüzde 10V ile karşılık bulmaktadır [70];

- ***Volume (Kapasite):*** Yüksek miktardaki veriyi ifade etmektedir.
- ***Velocity (Hız):*** Üretilen veri boyutunun kısa sürede çok yüksek olmasıdır.
- ***Variety (Çeşitlilik):*** Yapısal, yapısal olmayan ve yarı yapısal veri türleridir.
- ***Value (Değer):*** Bilinmeyen değerin ortaya çıkartılmasını sağlamaktadır.
- ***Veracity (Geçerlilik):*** Toplanan veriden geçerli olanın ayrılmasıdır.
- ***Variability (Değişkenlik):*** Farklı kaynaklardan farklı formatlarda veri toplanmasıdır.
- ***Validity (Doğrulanmışlık):*** Toplanan verinin doğrulandıktan sonra kullanılmasıdır.
- ***Vulnerability (Güvenlik Açığı):*** Büyük miktardaki veri kötü amaçlı kullanımlara açıktır.
- ***Volatility (Uçuculuk):*** Hızlıca kullanılmazsa değerini kaybedebilecek veriler içermektedir.
- ***Visualization (Görsellik):*** Standart görselleştirme araçları yetersiz kaldığından büyük veriye özgü görselleştirme uygulamalarını ifade etmektedir.

"V" harfleriyle özdeşleştirilen büyük veri kavramı aslında teknolojik bir terimden ziyade günden güne değişen dinamik yapıdaki bir teknolojik "yaklaşım" ya da "konsept" olarak karşımıza çıkmaktadır. 2000'li yılların başlarında ortaya atılan "3 Boyutlu Veri Yönetimi (Volume, Velocity, Variety)" yaklaşımı ile gelecekte veri yönetimine nasıl bakılacağı ortaya konmuştur [71]. Sonraki yıllarda hem akademik camia hem de bilişim endüstrisi bu yaklaşımı benimsemiştir. Büyük veri alanında yüzbinlerce akademik yayın yapılırken çok sa-

yıda bilişim projesi de hayata geçirilmiştir. Teknolojik yeniliklere göre büyük veri yaklaşımı da özellikle "veri bilimi" alanındaki popüler terimlerle birlikte yeni "V" harfleriyle ifade edilmeye devam etmiştir. Örneğin "victual (erzak)" ile veri biliminin beslendiği ana kaynak, "viability (yaşayabilirlik)" ile büyük verinin tek başına yaşayabilecek bir teknoloji olmadığı diğer teknolojilerle entegre edilmesi gerektiği, "vogue (moda)" ile büyük verinin teknoloji dünyasının moda trendlerinden birisi olduğu ifade edilmekte ve bu "V" sayısının toplamda 42'ye kadar çıktığı ve gelecekte yeni gelişmelerle daha da artacağı görüşü ileri sürülmektedir [72].

Büyük veri (big data) yaklaşımı verinin toplanmasını, yönetilmesini, analiz edilmesini ve bu veriye yönelik özel uygulamalar geliştirilmesi hayat döngüsünü içermektedir [73]. Sadece verinin kendisi büyük verinin uygulama alanı olarak kabul edilmemektedir. Büyük verinin işlenerek kıymetlendirilmesi sürecindeki tüm bileşenler büyük verinin ilgi alanına girmektedir. Donanım platformları, bulut bilişim çözümleri, güvenlik önlemleri, mahremiyet [74] ile ilgili kaygılar ve diğer birçok teknoloji büyük verinin çalışma alanı içindedir.

Özellikle açık kaynak istihbaratındaki veri boyutunun son on yılda yüksek miktarda artması bu verilerin klasik yaklaşımlarla işlenmesi ve analiz edilmesini imkânsız kılmaktadır. 2008 yılında Lockheed Martin firması tarafından geliştirilen Entegre Kriz Erken Uyarı Sistemi (Integrated Crisis Early Warning System - ICEWS) [75] yüzlerce farklı açık kaynaktan anlık veri toplayarak dünyanın farklı bölgelerinde bir toplumsal hareketlilik durumunu tespit edebilmektedir. Sistem açık kaynak istihbaratı ve büyük veri (OSINT – Big Data) yaklaşımlarının başarıyla uygulandığı bir proje olarak kabul edilmektedir [76].

Büyük verinin yaygınlaştığı bir dönemde açık kaynak istihbaratı ile birlikte tasarlanmış sistemlerin hayata geçirilmesi yenilikçi bir yaklaşımdan ziyade ciddi bir ihtiyaç olarak görülmektedir. Ancak tamamen insan unsurundan uzak kurulan açık kaynak tabanlı otomatize edilmiş büyük veri platformlarının başarılı olamayacağı değerlendirilmektedir. Büyük veriye dayalı etkili bir açık kaynak istihbaratı ekosistemi kurulabilmesi için mevcut teknolojilere ilaveten uzman analistlerin katkı sağlayabileceği insan unsurunun önemli bir bileşen olduğu tasarımların hayata geçirilmesi gerekmektedir [77].

Nesnelerin interneti (Internet of Things-IoT) cihazlarının günden güne artması ve yaygın kullanımlarıyla bu cihazların ürettikleri veri miktarı da büyü-

mektedir. Açık kaynak istihbaratı açısından internet bağlantısı olan ve gerekli güvenlik önlemleri alınmamış IoT cihazları ciddi bir kaynak oluşturmaktadır. Nesnelerin interneti cihazlarını tespit etmek ve açık kaynak istihbaratında kullanabilmek için "www.shodan.io" web sitesi üzerinden arama yapılabilmektedir.

Büyük Veri ve açık kaynak istihbaratını birlikte kullanmak politika yapıcılar, profesyoneller ve uygulayıcılar için oyun değiştirici olarak nitelendirilmektedir. Özellikle kamu güvenliği açısından kitlelerin genel eğilimi ve çevrimiçi radikalleşme aktivitelerinin tespiti büyük veri ve açık kaynak istihbaratı yaklaşımlarının sentezlenmesi ile mümkün olabilmektedir [78].

Büyük veri teknolojileri açısından gelişmiş demokratik ülkelerdeki eğilim daha çok kurumsal verinin kamuya açılması yönündedir. Bu açılımın daha şeffaf ve daha demokratik bir yönetim sistemini güçlendireceği görüşü benimsenmektedir [79]. Yeni gelişen büyük veri akımları açık kaynak istihbaratı açısından yeni fırsatlar doğurmaktadır.

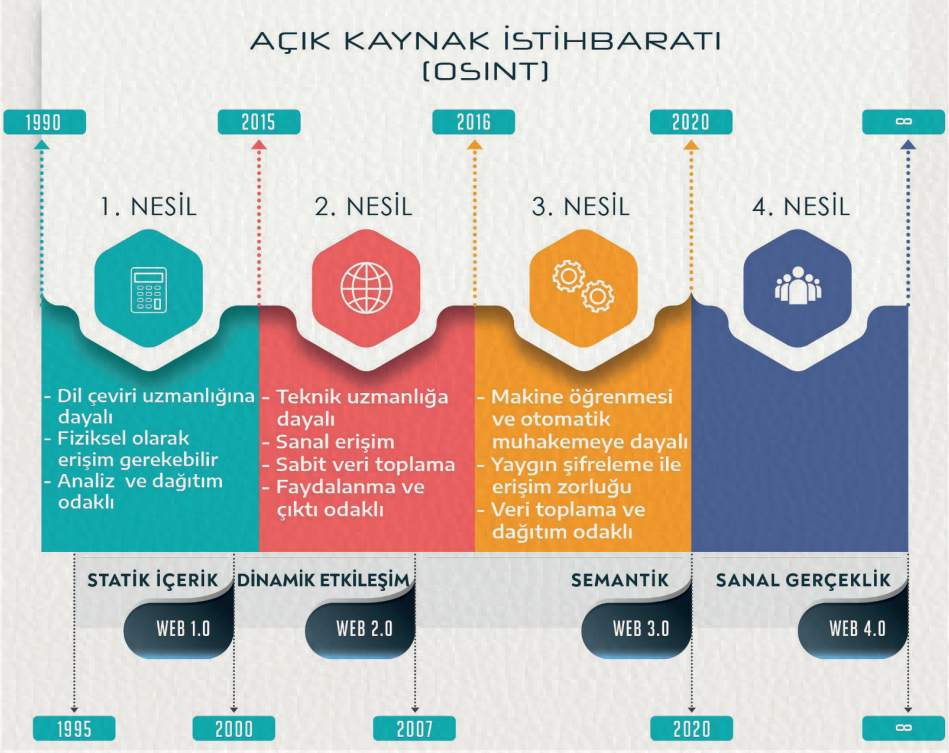
3.6. YAPAY ZEKÂ VE AÇIK KAYNAK İSTİHBARATI

En basit tanımıyla yapay zekâ (artificial intelligence-AI), görevleri yerine getirmek için insan zekâsını taklit eden ve topladıkları bilgilere göre yinelemeli olarak kendilerini iyileştirebilen sistemler veya makineler olarak ifade edilmektedir [80]. Büyük veriye dayalı 21. yüzyılın açık kaynak istihbaratının klasik yaklaşımlarla ve insan gücüyle sürdürülebilmesi artık tartışma dışı bir konudur. Açık kaynak istihbaratından toplanan verilerin analiz edilmesi ve kıymetlendirilebilmesi için başta makine öğrenmesi ve derin öğrenme gibi yapay zekâ algoritmalarının kullanılması bir tercihten öte zorunluluk hâlini almıştır.

Elli yıldan fazla geçmişi olduğu kabul edilen açık kaynak istihbaratı 1990'lı yıllardan itibaren internetle bağdaştırılmış bir olgu hâlini almıştır. Web teknolojilerindeki gelişmelere paralel olarak zaman içinde açık kaynak istihbaratı da doğrudan evrim geçirmiştir. Web 1.0 teknolojisinin geçerli olduğu dönemde 1. Nesil Açık Kaynak İstihbaratı (1st Generation OSINT), Web 2.0 teknolojisinin geçerli olduğu dönemde 2. Nesil Açık Kayak İstihbaratı (2nd Generation OSINT) ve Web 3.0 teknolojisinin artık kullanıldığı günümüzde 3. Nesil Açık Kaynak İstihbaratı (3rd Generation

OSINT) kabul gören sınıflandırmadır. Her dönemin kendine özgü açık kaynak istihbaratı toplama, işleme ve analiz etme yöntemleri vardır. 3. Nesil Açık Kaynak İstihbaratı (3rd Generation OSINT) tamamen başta makine öğrenmesi olmak üzere yapay zekâ algoritmalarına ve modern veri bilimi yaklaşımına dayanmaktadır [81].

Yapay zekâ algoritmaları ile açık kaynaklar üzerinden analiz yapılan en popüler platformlar yüzeysel webde hizmet veren sosyal medya servisleridir. Ancak içerik büyüklüğü açısından internet ekosisteminin çok küçük bir bölümünü oluşturan karanlık web sitelerinde dahi makine öğrenmesi ve derin öğrenme algoritmaları kullanılarak açık kaynak istihbaratı araştırmaları yapılmaktadır [82]. Aksi takdirde bu ağların klasik açık kaynak istihbaratı teknikleriyle izlenmesi ve analizler yapılması pratikte uygulanabilir görünmemektedir [83].



Şekil 3.14. Açık Kaynak İstihbaratının Zaman İçinde Değişimi

Özellikle birçok meslek grubunun yapay zekânın gelecekte ulaşabileceği seviyeye bağlı olarak ortadan kalkacağı ve insanların yapmakta olduğu birçok işin sadece robotlar tarafından yapılacağı ile ilgili öngörüler bulunmaktadır [84]. Aynı şekilde gelecekte açık kaynak istihbaratının tamamı olmasa da büyük bir kısmının yapay zekâya dayalı sistemler tarafından yapılacağını söylemek mümkündür.

3.7. STANDARTLAR VE PLATFORMLAR

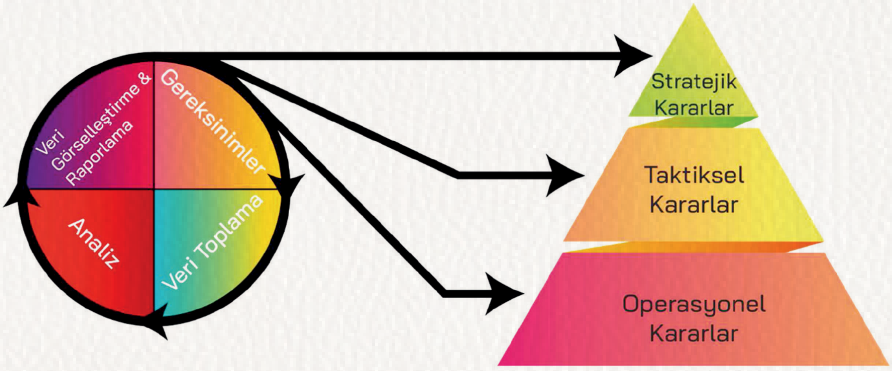
Bilgi değer zinciri olarak ifade edilen ham veriden organizasyonel sonuçlar elde etme sürecinde açık kaynak istihbaratı belli işlemlerin çıktısı olduğu gibi kendisinden sonra gelen karar verme adımının da girdisi konumundadır. Karar sözlük anlamında "bir iş veya sorun hakkında düşünülerek verilen kesin yargı" , karar verme ise "bir sorunu karara bağlamak, kararlaştırmak" olarak ifade edilmektedir [85]. Karar verme süreci bireysel bir kavram gibi gözükse de örgütsel açıdan da hayati öneme sahiptir. Yönetim bilimi açısından karar verme, en önemli yönetim faaliyetlerinden biri olarak, hareket tarzları içinde uygun seçeneğin belirlenmesi, yani organizasyonun istenilen sonuca ulaşması için alternatifler arasında seçim yapması olarak tanımlanmaktadır [86].

Bireysel karar verme ile örgütsel karar verme süreçleri arasındaki en büyük fark karar verme iradesinin delege edilmesi yani belli seviyedeki yöneticilere devredilmesidir [87]. Üst düzey yöneticiler stratejik kararlar, orta düzey yöneticiler taktiksel kararlar ve alt düzey yöneticiler ise operasyonel kararlar vermektedirler. Organizasyonların en iyi şekilde nasıl yönetilmesi gerektiği sorusuna cevap arayan stratejik yönetim araştırmalarının ilk odağı "bilgi akışı", ikincisi ise "karar verme" mekanizmalarıdır [88].

Endüstriyel anlamda açık kaynak istihbaratı açısından standart bir metodoloji bulunmamakla birlikte, stratejik yönetim anlayışı açısından açık kaynak istihbaratının standart metodolojisi karar verme süreçlerine yönelik bilgi akışı kapsamında şekillenmektedir. Açık kaynak istihbaratından elde edilen çıkarımlar sağlıklı bir bilgi akışı ile stratejik, taktiksel ve operasyonel karar verme süreçlerine yansımaktadırlar [89].

Açık kaynak istihbaratı konusunda akademik çalışmalar belli standartlar önermesinin yanı sıra bu alandaki sektör standartlarını, kurumsal destek ve danışmanlık hizmetleri de sunan bilgi güvenliği yazılımı şirketleri belirlemektedir [90].

Akademinin ve sektördeki uygulamaların standardizasyon konusunda kesiştiği nokta; gereksinimlerin belirlenmesi, verilerin toplanması, analiz edilmesi ve karar verme süreçlerine yönelik görsellerle desteklenen raporların oluşturulması olarak karşımıza çıkmaktadır [91].



Şekil 3.15. Açık Kaynak İstihbaratı Standartları - Stratejik Yönetim İlişkisi

Bir organizasyonun tüm açık kaynak istihbaratı gereksinimlerini karşılayabilecek bir platform bulunmamakla birlikte en kapsamlı olanı Maltego olarak karşımıza çıkmaktadır. Kurumsal seviyede üretilen açık kaynak istihbaratı platformlarının bir kısmı gizli kanallar üzerinden kamu kurumlarına satıldığından bu platformlarla ilgili detaylı bilgilere erişmek mümkün olmamaktadır.

Günümüzde birçok özel ve kamu kurumunun açık kaynak istihbaratı gereksiniminin büyük bir kısmını sosyal medya içerikleri oluşturmaktadır. Bu nedenle profesyonel sosyal medya analiz platformları açık kaynak istihbarat analiz platformları gibi kullanılmaktadır. Bu platformların bazıları yüzeysel web sitelerinden ve karanlık web sitelerinden de veri çekip analiz edebilmektedirler [92]. Sosyal medya analiz platformları özel şirketlerin sosyal medya takibi ve yönetimi ihtiyaçlarına cevap verdikleri gibi istihbarat servislerinin savunma ve güvenlik amaçlı açık kaynak istihbarat analizinde de sıklıkla tercih ettikleri bir model olarak kabul edilmektedir [93].

Açık kaynak istihbarat platformları kurumların kendi sunucu sistemlerinde veya son kullanıcı bilgisayarlarında çalışacak şekilde tasarlandığı gibi bulut bilişim alt yapısı üzerinden de çalışacak şekilde dizayn edilmektedir. Özellikle gizlilik ve mahremiyet açısından hassas konumda olmayan organizasyonlar

bulut bilişim alt yapıları üzerinde çalışan sosyal medya analiz platformlarını tercih etmektedirler. Bu konseptte hizmet veren platformlar özellikle sosyal medyanın devamlı gündemindeki hesaplara ait içerikler gibi ortak analiz edilecek verileri bir defa kaydetmekte ve tüm müşterilerin analizlerinde aynı veriyi kullanabilmektedir. Ayrıca ücretli servislere erişilmesi gereken açık kaynak istihbaratı süreçlerinde ortak kullanılan platformlar maliyet açısından daha uygun olmaktadır çünkü her müşteri için ayrı ayrı ücretli ödenmesi yerine platform üzerinden bu servis paylaştırılmaktadır.

3.8. AÇIK KAYNAK İSTİHBARATI PROJELERİ

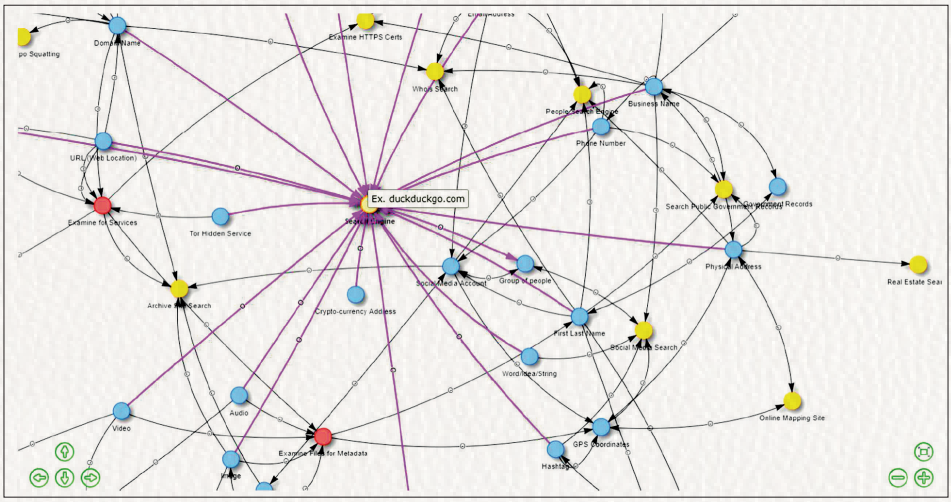
Açık kaynak istihbaratının doğası gereği bu alanda geliştirilen farklı projeler de aynı şekilde kamuya açık erişilebilir şekilde yayınlanmaktadır. Veriyi toplama, analiz etme ve raporlama amacıyla geliştirilen birçok araç farklı projeler altında toplanarak düzenli bir kullanım sağlamaktadır. Özellikle bilgi güvenliği alanında uzun yıllardır kullanılan açık kaynak istihbaratı araçlar yeni gelişen yazılım teknolojileri ile tekrar güncellenerek kullanılmaktadır.

Açık kaynak istihbaratı projelerinin bir kısmı kaynak kodları kapalı şekilde yayınlanırken [94] büyük bir kısmı ise açık kaynak kodlu olarak yayınlanmaktadır [95] böylece kullanıcılar bu projeleri kendi ihtiyaçları doğrultusunda geliştirip kullanabilmektedirler. Bireysel projelerin yanı sıra kamu kurumları da kaynak kodlarını paylaştığı projeler yayınlamaktadırlar. Fransa Uluslar Siber Güvenlik Ajansı tarafından geliştirilen Açık Siber Tehdit İstihbaratı Platformu (OPENCTI) [96] ve ABD Ulusal Coğrafi İstihbarat Ajansı tarafından geliştirilen Coğrafi İstihbarat Projesi (GEOINT) [97] açık kaynak kodlu olarak yayınlanmaktadır.

Uzun yıllardır geliştirilen açık kaynak istihbaratı projelerinin ilk örnekleri statik verilerin elde edilmesi ve basit çıkarımlar yapılmasına dayanırken güncel projeler daha çok akan verilerin anlık olarak toplanması ve hızla analiz edilmesi üzerine geliştirilmektedir. Bu durumda açık kaynak istihbaratının bir değer ifade edebilmesi için belli bir zaman diliminde sonuçlandırılması gerekmektedir aksi taktirde elde edilen veri güncelliğini ve dolayısıyla önemini yitirebilmektedir. Sürekli üretilen verinin hızlı bir şekilde kıymetlendirilebilmesi ve karar alma süreçlerine yansıtılabilmesi için klasik yazılım geliştirme yaklaşımları yerine yapay zekâ algoritmalarının kullanılması gerekmektedir.

Yapay zekâ algoritmalarına dayanan açık kaynak istihbaratı projelerinde yapılacak analizde aranacak kesinlik ve zaman maliyeti arasındaki denge gözetilmelidir. Yapay zekâ algoritmaları belli bir olasılık oranına göre başarılı kabul edilmektedir. Bu olasılığın yüksek olabilmesi için toplanan veri setinin de büyük olması gerekmektedir. Ayrıca ne kadar büyük veri seti toplanırsa bu verilerin işlenmesi ve analiz edilmesi de o derecede uzun olacaktır. Yani modelin başarılı olabilmesi için hem veri toplama hem de veri analiz etme süreçlerinde sistem kaynaklarına ve iletişim alt yapısına bağlı olarak daha fazla zamana ihtiyaç duyulacaktır. Bu durumda açık kaynak istihbaratı açısından gereksinimler ve beklentiler doğru yönetilerek süreci otomatikleştiren projelerden faydalanılmalıdır [98].

Adli ve idari birimler tarafından yönetilen açık kaynak istihbaratı süreçlerinin belki de en önemli aşaması tespit edilen bulguların resmî belgelere aktarılması olduğundan veri görselleştirme projeleri kamu görevlileri tarafından yoğunlukla kullanılmaktadır. Uluslararası güvenlik organizasyonları tarafından verilen eğitimlerde de açık kaynak istihbaratı görsel raporlama örnekleri paylaşılmaktadır.



Şekil 3.16. Açık Kaynak İstihbaratı Veri Görselleştirme Projesi Örneği [99]

Portekiz'deki Lisbon Üniversitesi [100] ve İngiltere'deki Londra Üniversitesi [101] ile beş bilgi güvenliği şirketinin konsorsiyumunda gerçekleştirilen ve 4 milyon avroluk bütçesinin 3.5 milyonunun Avrupa Birliği tarafından fon-

landığı "DiSIEM (Diversity Enhancements for Security Information and Event Management) Projesi [102]" adında açık kaynak istihbaratına dayalı siber tehdit istihbaratının merkeze alındığı bir alternatif bir bilgi güvenliği ve olay yönetim projesi (SIEM) geliştirilmiştir.

DiSIEM projesinin en büyük avantajı proje kapsamında yararlanılan açık kaynak istihbaratı araç ve tekniklerinin detaylı bir şekilde dokümante edilerek paylaşılmasıdır [103]. İlgili dokümanda proje kapsamında erişilerek veri çekilen sosyal medya platformları, standart web siteleri ile derin ve karanlık web sitelerinin tamamını listesi ve kullanım amaçları detaylı olarak belirtilmiştir. Ayrıca toplanan verilerin analiz edilmesi sürecinde hangi yapay zekâ algoritmalarının ve yöntemlerinin nasıl kullanıldığı da anlatılmıştır.

3.9. TEHDİT İSTİHBARATININ TEHDİT VE FIRSATLARI

Bir organizasyonun bilişim alt yapılarına yönelik siber tehditlerin tespit edilerek gerekli önlemlerin alınması hayati öneme sahiptir. Siber tehdit istihbaratı bir kurum veya kuruluşun bilişim sistemlerine karşı oluşan tehditle ilgili olarak; bu tehdit ve zararlı yazılımların kimin tarafından, hangi nedenle, kimi hedef aldığına dair çeşitli bilgilerin toplanarak, analiz edilmesi ve proaktif bir şekilde gerekli aksiyonların alınmasını ve iş birliği hâlindeki kurum ve kuruluşlarla elde edilen bilginin paylaşılmasını esas almaktadır [104].

Tehdit istihbaratı, birden fazla kaynak aracılığıyla, siber ortama yönelik tehditler hakkında bilgi toplamayı amaçlayan bir süreçtir. Olası olayların erken tespit edilebilmesi ve önlenebilmesi için elde edilen bilgilerin doğru analiz süreçlerinden geçirilerek kurumun güvenlik standartlarına uygun biçimde entegre edilmesi gerekmektedir. Tehdit istihbaratının kaynakları iç ve dış kaynaklar olmak üzere ikiye ayrılmaktadır [105]. İç kaynaklar kurum içi bilgiler iken dış kaynaklar kurum dışı bilgileri ifade etmektedir.

Şekil 3.17. Tehdit İstihbaratı ve Açık Kaynak İstihbaratı İlişkisi

Tehdit istihbaratının dış kaynaklarının bir kısmı kurumun iş birliği içinde olduğu diğer organizasyonlardan geldiği gibi bir kısmı da bu alanda ücretli hizmet sunan bilgi güvenliği şirketlerinden gelmektedir. Ancak dış kaynakların büyük bir kısmını açık kaynak istihbaratından elde edilebilen bilgiler içermektedir. Bu alanda ücretli servisler sunan bilgi güvenliği şirketlerinin de sunduğu hizmette elde ettiği verilerin büyük bir kısmı yine açık kaynaklardan gelmektedir. Profesyonel şirketler bu bilgileri toplayarak uzmanlıkları doğrultusunda düzenleyerek daha rafine bir şekilde kurumlara sunmaktadırlar [106].

Tehdit istihbaratının yarattığı en büyük fırsat tehditle henüz karşılaşmadan bilgi sahibi olunması ve gereken önlemlerin proaktif bir yaklaşımla alınmasıdır. Verilerin kolektif olarak toplanması makine öğrenmesi ve derin öğrenme tekniklerinin uygulanabildiği bir alan sağlamaktadır. Bilgi güvenliğinde bal küpü (honeypot) yöntemiyle siber alt yapıları hedef alan potansiyel saldırganlar tuzak sistemlere yönlendirilerek tespit edilen saldırı senaryosu tehdit istihbaratı süreçlerine eklenebilmektedir. Böylece daha bütüncül bir savunma stratejisi geliştirilebilmektedir [107]. Tehdit istihbaratı kamu kurumlarını korurken özel şirketleri de içinde bulundukları rekabet ortamında bir adım önde tutmaktadır.

Siber tehdit istihbaratı gelecek projeksiyonu yapılabilmesine de katkı yapmaktadır. Risklerin önceden belirlenmesi ve gelecek öngörülerine bağlı olarak kurumsal kaynakların daha doğru yönetilmesine imkân sağlanmaktadır. Özellikle ihtiyaç duyulabilecek personel [108] ve niteliklerinin belirlenmesinde, organizasyonun teknik imkân ve kabiliyetlerinin arttırılmasına yönelik yatırımların planlanmasında tehdit istihbaratı yönlendirici olacaktır.

Açık kaynak istihbaratının avantajları ve dezavantajları tehdit istihbaratına da aynı şekilde yansımaktadır. Hızlı, kapsamlı ve kolay bir istihbarat sağlanırken özellikle tamamen teyit edilmemiş bilgilerin istihbarat sürecine dâhil edilerek kullanılması beraberinde başka tehditleri getirmektedir. Uzman öngörüsünün ve insan elementinin dâhil edilmediği veri bilimine dayalı otomatik süreçler avantajdan çok dezavantajlı olabilmektedir [109]. Tehdit istihbaratına bağlı olarak otomatik aksiyon alınması gereken sistemler kurulurken profesyonel bilgi güvenliği şirketlerinin sunmuş

olduğu ve uzman denetiminden geçen platformların tercih edilmesi riski azaltacaktır [110].

Tehdit istihbaratı, istihbarat dünyasını içinde farklı bir seviyede değerlendirilmektedir. Bu seviyeye yükselebilmiş istihbarat servisleri diğer ülkeler için tehdit oluşturmaktadır. Aynı şekilde tehdit istihbaratını başarıyla uygulayabilen organizasyonlar ve firmalar rakipleri için tehdit anlamına gelmektedir [111].

Günümüzde tüm organizasyonların bir siber tehdit istihbaratı programı olması zorunlu hâle gelmiştir. Bu program çerçevesinde farklı organizasyonlar ve bilgi güvenliği oluşumlarının elde ettikleri kritik bilgileri karşılıklı paylaşmaları gerekmektedir. Siber tehdit istihbaratının sunduğu fırsatlardan birisi de organizasyonlar ve paydaşlar arasında istihbarat paylaşımını kolaylaştırmasıdır. Ancak bu fırsat beraberinde belli zorlukları da getirmektedir. Özellikle toplanan verilerin paylaşımı sonrası otomatik aksiyon alınması sürecinde verinin güvensizliği nedeniyle bir olumsuzluk yaşandığında kimin sorumlu olacağı tartışılmaktadır. Ayrıca çok kritik bir siber tehdit istihbaratını elde eden bir paydaş önce kendisi bu istihbarattan faydalanıp sonra mı paylaşacak yoksa aynı anda mı paylaşacağı diğer bir çözülmesi gereken problem olarak görülmektedir [112].

3.10. SONUÇ VE DEĞERLENDİRMELER

Açık kaynak istihbaratı günden güne önemini arttıran ve birçok farklı alanda uygulanması bir tercihten öte ihtiyaca dönüşen bir olgudur. Günümüzün en çok dikkat çeken teknolojik gelişmeleri olan büyük veri, yapay zekâ, bilgi güvenliği ve nesnelerin interneti gibi konuların yanında ülkemizde de hayata geçirilmesi amaçlanan "açık veri" vizyonu [113] ile birlikte düşünülmesi gereken kavram tartışmasız bir şekilde açık kaynak istihbaratıdır.

Özellikle demokratikleşme adımları ile gelişmiş ülkeleri yakalamayı hedefleyen ülkelerde devlet kurumları ve büyük organizasyonlar tarafından üretilen veriler araştırmacıların çalışmalarında kullanılmak üzere mahremiyete dikkat edilerek yayınlanmaktadır. Bağımsız bir kuruluş olan "World Wide Web Vakfı" tarafından yürütülen "Açık Veri Ölçeği Projesi (The Open Data Ba-

rometer) [114] ” kapsamında, hükümetlerin hesap verilebilirlik, şeffaflık ve yeniliklere açıklık durumları açısından verilerini açık kaynaklardan ne kadar yayınladıkları ölçülmekte ve sıralanmaktadır.

Sınırların kalktığı, ülkelerin siyasi, ekonomik ve güvenlik konularında giderek daha iç içe girmeye başladığı yeni dünya düzeninde kamu güvenliği küçük büyük her ülke için en kritik bir mesele hâlini almıştır. Böyle bir dönemde hem genel kamu güvenliğinde hem de özellikle terörle mücadele alanında hükümetlerin ellerindeki tüm enstrümanları sonuna kadar kullanmaları gerekmektedir. İstihbarat toplama süreçlerinde açık kaynaklar gibi izin gerektirmeyen risksiz kanallar varken [115] başka hedeflere yönelmek rasyonel olmayacaktır. Aynı stratejiyi kâr amacı güden şirketler de benimsemeli, rakipleri ve piyasa hakkında bilgi toplamaları gereken durumlarda açık kaynakları kullanmalıdır.

Üniversiteler her kademedeki öğrencilerine ve araştırmacılara açık kaynak istihbaratını akademik perspektifte nasıl kullanılabileceğini muhakkak anlatmalı ve devamlı gündeminde tutmalıdır. Akademik araştırma metodolojisi ile açık kaynak istihbaratı metodolojisi sentezlenerek, yapay zekâ ve veri analitiği teknikleri ile birlikte bilimsel çalışma yapma alışkanlığı benimsenmelidir.

Açık kaynak istihbaratı eğitimden sağlığa, tarımdan hayvancılığa, ekonomiden siyasete kadar devletlerin temel ilgi alanlarında uygulanabilecek bir yöntemdir. Bu alanlarda dünyadaki gelişmeleri takip etmek, yarış içinde olduğu alanlarda komşularının durumlarını analiz etmek için farklı alan uzmanlıklarına sahip yetişmiş personelden oluşan özel birimler kurulmalı ya da mevcut kurumlar bu bakış açısıyla yönlendirilmelidir.

Her gün katlanarak artan açık kaynaklardan erişilebilen verilerin değerini anlayan ve buna göre strateji geliştiren kişi, kurum ya da organizasyonlar geleceğin kazananları olacaktır. Çünkü her tür ve formatta bilgiye ulaşmanın giderek kolaylaştığı çağımızda veri yeni petrol olarak tanımlanmakta ve bu petrolü toprağın altından çıkarma zorunluluğu bulunmamaktadır. Adeta her milisaniyede topraktan çıkarak fışkırırcasına bilgi açık kaynaklarda akmaktadır. Bu bilgiyi işleme ve analiz etme kabiliyeti uzunca bir süre 21. yüzyılın ana kuvvet çarpanı olacaktır.

KAYNAKLAR

[1] Türk Dil Kurumu Sözlükleri, https://sozluk.gov.tr, Son Erişim Tarihi: 17.04.2020

[2] Kamu Düzeni ve Güvenliği Müsteşarlığı, "Güvenlik Terimleri Sözlüğü", 2017, Ankara, İmak Ofset Basım Yayın,

[3] Intelligence noun - Definition, pictures, pronunciation and usage notes | Oxford Advanced Learner's Dictionary at OxfordLearnersDictionaries.com, https://www.oxfordlearnersdictionaries.com/definition/english/intelligence, Son Erişim Tarihi: 17.04.2020

[4] Competing in the Knowledge Economy: The Knowledge Value Chain (KVC) » Knowledge Value Chain®, http://www.knowledgevaluechain.com/home, Son Erişim Tarihi: 17.04.2020

[5] Özdağ, Ümit, 2014, "İstihbarat Teorisi", Ankara, Kripto Basım Yayın Dağıtım

[6] Fidan, Hakan, 1999, "Intelligence and foreign policy: A comparison of British, American and Turkish intelligence systems", İhsan Doğramacı Bilkent Üniversitesi / Sosyal Bilimler Enstitüsü / Uluslararası İlişkiler Anabilim Dalı, Y.L. Tezi

[7] Özdağ, 2014, a.g.e.

[8] What is Grey Literature? | Grey Literature Database, http://www.greylit.org/about, Son Erişim Tarihi: 17.04.2020

9] Open Source Intelligence: Professional Handbook, 1996, Joint Military Intelligence Training Center, http://www.oss.net/dynamaster/file_archive/080807/a3127ddeaa9a083affdddce6766401fc/Open%20Source%20Intelligence_Professional%20Handbook.pdf, Son Erişim Tarihi: 17.04.2020

[10] Friedman, Richard S., 2005, "Open Source Intelligence: A Review Assay", Intelligence and the National Security Strategist: Enduring Issues and Challenges, Ed. Kline, Robert D. & George, Roger Z., ABD, Rowman & Littlefield Pubishers, sayfa 285

[11] Benavides, Ben, 2015, "Open Source Intelligence 2oolKit On the Go", https://osint.co.nz/wp-content/uploads/2018/09/2016-OSINT-2oolKit-Benavides.pdf, Son Erişim Tarihi: 17.04.2020

[12] Jardines, Elliot A., 2002, "Theory and History of OSINT Understanding Open Sources", NATO Osint Intelligence Reader, http://www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546bf5c9f1ed/ NATO%20OSINT%20Reader%20FINAL%2011OCT02.pdf, Son Erişim Tarihi: 17.04.2020

[13] Çıtak, Emre, 2016, "Çağımızın Gerekliliği Olarak Sinyal İstihbaratı", Hitit Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, Yıl 8, Sayı 2

[14] Ünver, H. Akın, 2018, "Dijital Açık Kaynaklı İstihbarat ve Uluslararası Güvenlik", Siber Politikalar ve Dijital Demokrasi, Edam — Ekonomi ve Dış Politika Araştırma Derneği, https://edam.org.tr/dijital-acik-kaynakli-istihbarat-ve-uluslararasi-guvenlik, Son Erişim Tarihi: 07.04.2020

[15] Glassman, Michael ve Kang, Min Ju, 2012, "Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT)", Computers in Human Behavior, Cilt 28, Sayı 2, sayfa 673-682

[16] Apple, Edward J., 2014, "Cybervetting Internet Searches for Vetting, Investigations, and Open-Source Intelligence, Second Edition", ABD, CRC Press Taylor & Francis Group

[17] Engebretson, Patrick, 2013, "Chapter 2 - Reconnaissance", Ed. Patrick Engebretson, The Basics of Hacking and Penetration Testing (Second Edition), Syngress, sayfa 19-51,

[18] Miller, Bowman H., 2018, "Open Source Intelligence (OSINT): An Oxymoron?", International Journal of Intelligence and CounterIntelligence, Cilt 31, Sayı4, Sayfa 702-719, DOI:10.1080/08850607.2018.1492826

[19] [Hribar, Gašper, Podbregar, Iztok ve Teodora Ivanuša, 2014, "OSINT: A Grey Zone?", International Journal of Intelligence and CounterIntelligence, Cilt 27, Sayı 3, Sayfa 529-549, DOI: 10.1080/08850607.2014.900295

[20] Wheatley, Ben, 2018, "British open source intelligence (OSINT) and the Holocaust in the Soviet Union: persecution, extermination and partisan warfare", Intelligence and National Security, Cilt 33, Sayı 3, Sayfa 422-438, DOI: 10.1080/02684527.2017.1410516

[21] Pringle, Robert W., 2003, "The Limits of OSINT: Diagnosing the Soviet Media, 1985-1989", International Journal of Intelligence and CounterIntelligence, Cilt 16, Sayı 2, Sayfa 280-289, DOI: 10.1080/08850600390198706

[22] Calkins , Laura M., 2011, "Patrolling the Ether: US–UK Open Source Intelligence Cooperation and the BBC's Emergence as an Intelligence Agency, 1939–1948", Intelligence and National Security, Cilt 26, Sayı 1, Sayfa 1-22, DOI: 10.1080/02684527.2011.556355

[23] Yates, Athol ve Zvegintzov, Nicholas, 1999, "A Siberian reality check on open source information", The Australian Library Journal, Cilt 48, Sayı 4, Sayfa 343-357, DOI: 10.1080/00049670.1999.10755895

[24] Özer, Nuri P., 2019, "Propagandada Yöntemler, Araçlar Ve Bir Propaganda Modeli Olarak; Herman Ve Chomsky Propaganda Modeli", Kritik İletişim Çalışmaları Dergisi , Cilt 1, Sayı 1, Sayfa 15-30

[25] World Internet Users Statistics and 2020 World Population Stats, https://www.internetworldstats.com/stats.htm, Son Erişim Tarihi: 17.04.2020

[26] Hobbs C., Moron M., Salisbury D., 2014, "Introduction", Ed. Hobbs C., Moran M., Salisbury D., Open Source Intelligence in the Twenty-First Century. New Security Challenges, Londra, Palgrave Macmillan

[27] Jones, Emily, 2018, "Artificial Intelligence in 2018 – Taking our Jobs, or Creating New Ones?", https://www.sitepronews.com/2018/02/05/artificial-intelligence-2018-taking-jobs-creating-new-ones, Son Erişim Tarihi: 17.04.2020

[28] Paterson A., Chappell J., 2014, "The Impact of Open Source Intelligence on Cybersecurity". Ed. Hobbs C., Moran M., Salisbury D., Open Source Intelligence in the Twenty-First Century. New Security Challenges, Londra, Palgrave Macmillan

[29] "Cyber Bites <Open Source Intelligence (OSINT) Introduction>" Eğitim Notları, CEPOL | European Union Agency for Law Enforcement Training, Avrupa Birliği Kolluk Kuvetleri Eğitim Ajansı, E-Net Çevrimiçi Eğitim Portalı, https://enet.cepol.europa.eu, Son Erişim Tarihi: 17.04.2020

[30] Kumar, Srijan, Cheng, Justin, Leskovec, Jure ve Subrahmanian, V.S., 2017, "An Army of Me: Sockpuppets in Online Discussion Communities". WWW '17: Proceedings of the 26th International Conference on World Wide Web, Nisan 2017 Sayfa 857–866, DOI: 10.1145/3038912.3052677.

[31] The Intelligence Cycle — Central Intelligence Agency (ABD – Merkezi İstihbarat Teşkilatı), https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence-cycle.html, Son Erişim Tarihi: 17.04.2020

[32] Altheide, Cory ve Carvey, Harlan, 2011, "Digital Forensics with Open Source Tools", Syngress, USA

[33] Agate M. Ponder-Sutton, 2016, "Chapter 1 - The Automating of Open Source Intelligence", Editörler: Robert Layton, Paul A. Watters, Automating Open Source Intelligence, Syngress, Sayfa 1-20, 10.1016/B978-0-12-802916-9.00001-4

[34] Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution, https://www.kali.org, Son Erişim Tarihi: 17.04.2020

[35] Buscador OSINT VM, https://inteltechniques.com/buscador, Son Erişim Tarihi: 17.04.2020

[36] Maltego, https://www.maltego.com, Son Erişim Tarihi: 17.04.2020

[37] Chauhan, Sudhanshu ve Panda, N. Kumar, 2015, "Hacking Web Intelligence Open Source Intelligence and Web Reconnaissance Concepts and Techniques", ABD, Syngress, Sayfa 124, DOI: 10.1016/C2014-0-00876-3

[38] Metin Madenciliği (Text Mining) Nedir, http://www.metinmadenciligi.com/, Son Erişim Tarihi: 30.05.2020

[39] Akbıyık, Adem, 2019, "Sosyal Bilimlerde Metin Madenciliği Wordstat Uygulamaları", Sakarya, Sakarya Yayıncılık

[40] Gabrielatos, Costas, 2018. "Keyness analysis: Nature, metrics and techniques", Ed. Taylor, C. & Marchi, A., Corpus Approaches To Discourse: A critical review. Oxford: Routledge., Bölüm: 11, Routledge, sayfa.225-258

[41] Granger, Sylviane, 1998, "Prefabricated patterns in advanced EFL writing: collocations and formulae", Ed. A.P. Cowie, Phraseology: theory, analysis and applications, Oxford University Press, sayfa.145-160

[42] Berisha V, Wang S, LaCross A, Liss J. 2015, "Tracking discourse complexity preceding Alzheimer's disease diagnosis: a case study comparing the press conferences of Presidents Ronald Reagan and George Herbert Walker Bush", J Alzheimers Dis. Cilt: 45, Sayı: 3, Sayfa: 959-963, DOI:10.3233/JAD-142763

[43] Al-Natour, Sameh ve Turetken, Ozgur, 2020, "A comparative assessment of sentiment analysis and star ratings for consumer reviews", International Journal of Information Management, Cilt 54, Sayı 102132, DOI: 10.1016/j.ijinfomgt.2020.102132.

[44] Danowski, J.A., 2012, "Sentiment Network Analysis of Taleban and RFE/RL Open-Source Content about Afghanistan", 2012 European Intelligence and Security Informatics Conference, 303-310, 22-24 Ağustos 2012, Odense, Danimarka DOI: 10.1109/EISIC.2012.54.

[45] Steketee, Michael ve Atsushi Miyaoka, Maura Spiegelman, 2015, "Social Network Analysis", Ed. James D. Wright, International Encyclopedia of the Social & Behavioral Sciences (Second Edition), Elsevier, Sayfa 461-467, DOI: 10.1016/B978-0-08-097086-8.10563-X.

[46] Holland, Benjamin Robert, 2012, "Enabling Open Source Intelligence (OSINT) in Private Social Networks", Y.L. Tezi, Iowa State University

[47] NodeXL | Your Social Network Analysis Tool for Social Media, https://www.smrfoundation.org/nodexl/, Son Erişim Tarihi: 31.05.2020

[48] Hansen, Derek L ve Ben Shneiderman, Marc A. Smith, Itai Himelboim, 2011, "Chapter 1 - Introduction to social media and social networks", Ed. Derek L. Hansen, Ben Shneiderman, Marc A. Smith, Itai Himelboim, Analyzing Social Media Networks with NodeXL (Second Edition) Morgan Kaufmann, Sayfa: 3-10, DOI: 10.1016/B978-0-12-817756-3.00001-7.

[49] Hansen, Derek L. ve Ben Shneiderman, Marc A. Smith, 2011, "Chapter 3 - Social Network Analysis: Measuring, Mapping, and Modeling Collections of Connections", Ed. Derek L. Hansen, Ben Shneiderman, Marc A. Smith, Analyzing Social Media Networks with NodeXL, Morgan Kaufmann, Sayfa: 31-50, DOI: 10.1016/B978-0-12-382229-1.00003-5.

[50] Scott, John ve Frans N. Stokman, 2015, "Social Networks", Ed. James D. Wright, International Encyclopedia of the Social & Behavioral Sciences (Second Edition), Elsevier, Sayfa 473-477, DOI: 10.1016/B978-0-08-097086-8.32101-8.

[51] Weyers, Jeff R. ve Camie Condon, "New Zealand Jihadist Deletes Tweets after Discovering he left Geotagging On", https://ibrabo.wordpress.com/2014/12/30/new-zealand-jihadist-deletes-tweets-after-discovering-he-left-geotagging-on/, Son Erişim Tarihi: 31.05.2020

[52] Art. 4 GDPR - Definitions - GDPR.eu, https://gdpr.eu/article-4-definitions/, Son Erişim Tarihi: 31.05.2020

[53] Safi, Michael, 2015, "New Zealander thought to be fighting in Syria accidentally tweets locations | World news | The Guardian", https://www.theguardian.com/world/2015/jan/01/new-zealander-syria-isis-accidentally-tweets-locations, Son Erişim Tarihi: 31.05.20 20

[54] Swannie, Karl, 2018, "Why The Best OSINT Tools Use Geofencing Technology", https://www.echosec.net/blog/osint-tools, Son Erişim Tarihi: 31.05.2020

[55] Condon, Camie ve Weyers, Jeff, 2019, "Where The Bodies are Buried: Geolocating The Execution Site Linked To A Canadian Isis Commander", https://ibrabo.files.wordpress.com/2019/01/ibrabo-where-the-bodies-are-buried.pdf, Son Erişim Tarihi: 31.05.2020

[56] SunCalc - Sun Calculator Photovoltaic System, https://www.suncalc.org/, Son Erişim Tarihi: 31.05.2020

[57] Bertram, Stewart K., 2015, "The Tao of Open Source Intelligence", Birleşik Krallık, IT Governance Publishing

[58] Tor Project | Anonymity Online, https://www.torproject.org, Son Erişim Tarihi: 17.04.2020

[59] Freenet, https://freenetproject.org, Son Erişim Tarihi: 17.04.2020

[60] I2P Anonim Ağı, https://geti2p.net/tr/, Son Erişim Tarihi: 17.04.2020

[61] INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2019 | Europol, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019, Son Erişim Tarihi: 17.04.2020

[62] EU Terrorism Situation ve Trend Report (Te-Sat) | Activities & Services | Main Reports | Europol, https://www.europol.europa.eu/tesat-report, Son Erişim Tarihi: 17.04.2020

[63] Negi, Neelam, 2017, "Comparison of Anonymous Communication Networks-Tor, I2P, Freenet", International Research Journal of Engineering and Technology (IRJET), Cilt 4, Sayı 7

[64] Bartlett, Jamie, 2016, "Dark Net :İnternetin Yeraltı Dünyası", İstanbul, Timaş Yayınları

[65] Tor Metrics, https://metrics.torproject.org, Son Erişim Tarihi: 14.04.2020

[66] Kaur, S. ve Randhawa, S., 2020, "Dark Web: A Web of Crimes", Wireless Personal Communications, DOI: 10.1007/s11277-020-07143-2

[67] WorldWideWebSize.com | The size of the World Wide Web (The Internet), https://www.worldwidewebsize.com, Son Erişim Tarihi: 17.04.2020

[68] "Darknet" Eğitim Notları, CEPOL | European Union Agency for Law Enforcement Training, Avrupa Birliği Kolluk Kuvetleri Eğitim Ajansı, E-Net Çevrimiçi Eğitim Portalı, https://enet.cepol.europa.eu, Son Erişim Tarihi: 17.04.2020

[69] Terzi, Ramazan, 2017, "Büyük Veri ve Açik Veri: Temel Kavramlar", Ed. Prof. Dr. Şeref Sağıroğlu, Dr. Orhan Koç Büyük Veri ve Açık Veri Analitiği: Yöntemler ve Uygulamalar, Ankara, Grafiker Yayınları

[70] Khan, Nawsher, Alsaqer, Mohammed, Shah, Habib, Badsha, Gran, Abbasi, Aftab ve Salehian, Solmaz, 2018, "The 10 Vs, Issues and Challenges of Big Data", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Cilt 3, Sayı 5, sayfa 52-56. DOI: 10.1145/3206157.3206166.

[71] Lancy, Dough, 2001, "3d Data Management: Controlling Data Volume, Velocity and Variety", https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf, Son Erişim Tarihi: 20.05.2020

[72] Shafer, Tom, 2017, "The 42 V's of Big Data and Data Science", https://www.elderresearch.com/blog/42-v-of-big-data, Son Erişim Tarihi: 20.05.2020

[73] Hong, Shu, 2016, "Big data analytics: six techniques", Geo-spatial Information Science, Cilt 19, Sayı 2, Sayfa 119-128, DOI: 10.1080/10095020.2016.1182307

[74] Sağıroğlu, Şeref ve Canbay, Yavuz ve Vural, Yılmaz, 2017, "Büyük Veri Mahremiyetinde Kullanılan Kavramlar ve Yöntemler", Ed. Prof. Dr. Şeref Sağıroğlu, Dr. Orhan Koç Büyük Veri ve Açık Veri Analitiği: Yöntemler ve Uygulamalar, Ankara, Grafiker Yayınları

[75] ICEWS | Lockheed Martin, https://www.lockheedmartin.com/en-us/capabilities/research-labs/advanced-technology-labs/icews.html, Son Erişim Tarihi: 17.04.2020

[76] Senekal Burgert ve Kotzé, Eduan, 2019, "Open source intelligence (OSINT) for conflict monitoring in contemporary South Africa: Challenges and opportunities in a big data context", African Security Review, Cilt 28, Sayı 1, Sayfa 19-37, DOI: 10.1080/10246029.2019.1644357

[77] Christopher Eldridge, Christopher Hobbs ve Matthew Moran, (2018), "Fusing algorithms and analysts: open-source intelligence in the age of 'Big Data'", Intelligence and National Security, 33:3, 391-406, DOI: 10.1080/02684527.2017.1406677

[78] Staniforth, Andrew, 2016, "Open Source Intelligence and the Protection of National Security", Ed. Babak Akhgar, P. Saskia Bayerl, Fraser Sampson, Open Source Intelligence Investigation From Strategy to Implementation, İsviçre, Springer, DOI: 10.1007/978-3-319-47671-1_2.

[79] Sağıroğlu, Şeref, 2017, "Büyük Veri Dünyasi: Büyük Veri Büyük Etki", Ed. Prof. Dr. Şeref Sağıroğlu, Dr. Orhan Koç Büyük Veri ve Açık Veri Analitiği: Yöntemler ve Uygulamalar, Ankara, Grafiker Yayınları

[80] Yapay Zekâ Nedir?, https://www.oracle.com/tr/artificial-intelligence/what-is-artificial-intelligence.html, Son Erişim Tarihi: 17.04.2020

[81] Williams, Heather J. ve Ilana Blum, 2018, "Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise". Santa Monica, CA: RAND Corporation, https://www.rand.org/pubs/research_reports/RR1964.html. Son Erişim Tarihi: 17.04.2020

[82] Jaspal, Kaur Saini ve Divya, Bansal, 2019, "A Comparative Study and Automated Detection of Illegal Weapon Procurement over Dark Web", Cybernetics and Systems, Cilt 50, Sayı 5, Sayfa: 405-416 DOI: 10.1080/01969722.2018.1553591

[83] Nabki, M.W., Fidalgo, E., Alegre, E. ve Chaves, D., 2019, "Content-Based Features to Rank Influential Hidden Services of the Tor Darknet", ArXiv, abs/1910.02332.

[84] Say, Cem, 2020, "50 Soruda Yapay Zekâ", İstanbul, 7 Renk Basım Yayın ve Fimcilik

[85] Türk Dil Kurumu Sözlükleri, https://sozluk.gov.tr/?kelime=karar%20vermek, Son Erişim Tarihi: 26.05.2020

[86] Özer, M. Akif, 2012, "Örgütsel Karar Verme ve Yönetişim", Türk İdare Dergisi, Sayı: 475, Sayfa: 147-170

[87] Yaşar, Okan, 2016, "Davranışsal Karar Verme: Düşünme, Problem Çözme", Ankara, Detay Yayıncılık

[88] Çelikten, Mustafa ve Fahrettin Gılıç, Yeliz Çelikten, Ahmet Yıldırım, 2019, "Örgüt Yönetiminde Karar Verme Süreci: Bitmeyen Bir Tartışma", Mersin Üniversitesi Eğitim Fakültesi Dergisi, Cilt: 15, Sayı: 2, Sayfa: 581-592

[89] Doerr, Christian, 2018, "Cyber Threat Intelligence Standards - A high-level overview", The European Union Agency for Cybersecurity (ENISA) - 2018 CTI-EU | Bonding EU Cyber Threat Intelligence Çalıştayı, https://www.enisa.europa.eu/events/2018-cti-eu-event/cti-eu-2018-presentations/cyber-threat-intelligence-standardization.pdf, Son Erişim Tarihi: 26.05.2020

[90] Open-Source Intelligence (OSINT) Gathering Training | SANS SEC487, https://www.sans.org/course/open-source-intelligence-gathering, Son Erişim Tarihi: 26.05.2020

[91] Pastor-Galindo, Javier ve Nespoli, Pantaleone & Gomez Marmol, Felix & Martinez Perez, Gregorio, 2020, "The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends", IEEE Access, Cilt 8, Sayfa: 10282-10304, DOI: 10.1109/ACCESS.2020.2965257.

[92] Medusa - OSINT Platform, https://www.medusa-labs.com/, Son Erişim Tarihi 27.05.2020

[93] Brelsford, Paul, 2014, "Employing a social media monitoring tool as an OSINT platform for Inte]lligence, Defence & Security", The #1 Social Media Analytics & Monitoring Platform – Talkwalker.com, https://www.slideshare.net/AlesJohn/employing-social-media-monitoring-tools-as-an-osint-platform-for-intelli, Son Erişim Tarihi: 27.05.2020

[94] Google Hacking Diggity Project – Bishop Fox, https://resources.bishopfox.com/resources/tools/google-hacking-diggity/attack-tools/, Son Erişim Tarihi: 01.06.2020

[95] ElevenPaths/FOCA: Tool to find metadata and hidden information in the documents, https://github.com/ElevenPaths/FOCA, Son Erişim Tarihi: 01.06.2020

[96] OpenCTI - Open platform for cyber threat intelligence, https://www.opencti.io/en/, Son Erişim Tarihi: 31.05.2020

[97] National Geospatial-Intelligence Agency, https://github.com/ngageoint, Son Erişim Tarihi: 31.05.2020

[98] Weir, George R.S., 2016, "Chapter 9 - The Limitations of Automating OSINT: Understanding the Question, Not the Answer", Ed. Robert Layton, Paul A. Watters, Automating Open Source Intelligence, Syngress, Sayfa: 159-169, DOI: 10.1016/B978-0-12-802916-9.00009-9.

[99] OSINT YOGA, https://yoga.osint.ninja/, Son Erişim Tarihi: 01.06.2020

[100] Faculdade de Ciências da Universidade de Lisboa, https://ciencias.ulisboa.pt/en/, Son Erişim Tarihi: 01.06.2020

[101] City, University of London, https://www.city.ac.uk/, Son Erişim Tarihi: 01.06.2020

[102] DiSIEM Project, http://disiem-project.eu/, Son Erişim Tarihi: 01.06.2020

[103] Ferreira, Pedro M., 2018, "Disiem D4.1 Techniques and tools for OSINT-based threat analysis", http://disiem-project.eu/wp-content/uploads/2018/06/D4.1v2.pdf, Son Erişim Tarihi: 01.06.2020

[104] Yelken, Anıl Baran, 2019, "Siber Tehdit İstihbaratı – CyberMag", https://www.cybermagonline.com/siber-tehdit-istihbarati, Son Erişim Tarihi: 01.06.2020

[105] Zor, Rafet, 2020, "Tehdit İstihbaratı Nedir?", https://www.pwc.com.tr/tr/assets/pdf/tehdit-istihbarati.pdf, Son Erişim Tarihi: 01.06.2020

[106] Kaspersky Threat Intelligence, https://media.kaspersky.com/en/business-security/enterprise/Kaspersky_Threat_Intelligence_Services.pdf, Son Erişim Tarihi: 02.06.2020

[107] Conti M., Dargahi T., Dehghantanha A., 2018, "Cyber Threat Intelligence: Challenges and Opportunities", Ed. Dehghantanha A., Conti M., Dargahi T., Cyber Threat Intelligence. Advances in Information Security, Cilt 70. Springer, Cham

[108] Arıkan, Süleyman Muhammed, 2019, "Veri Madenciliği Temelli Siber Tehdit istihbaratı", Y.L. Tezi, Gazi Üniversitesi, Bilişim Enstitüsü, Adli Bilişim Anabilim Dalı

[109] Knopp, Bradley ve Sina Beaghley, Aaron Frank, Rebeca Orrie, Michael Watso, 2016, "Defining the Roles, Responsibilities, and Functions for Data Science Within the Defense Intelligence Agency", RAND Corporation, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1500/RR1582/RAND_RR1582.pdf, Son Erişim Tarihi: 02.06.2020

[110] Threat Intelligence: Definiton, Benefits, Use Cases & Examples, https://www.crowdstrike.com/epp-101/threat-intelligence/, Son Erişim Tarihi: 02.06.2020

[111] Wesley. Michael, 2004, "New frontiers of intelligence analysis: shared threats, diverse perspectives, new communities" Konferansı, Roma, İtalya, 31 Mart-2 Nisan 2004

[112] Wagner, Thomas D. ve Khaled Mahbub, Esther Palomar, Ali E. Abdallah, 2019, "Cyber threat intelligence sharing: Survey and research directions", Computers & Security, Cilt 87, Sayı: 101589, DOI: 10.1016/j.cose.2019.101589.

[113] AçıkVeri Projesi - Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi - Proje Açıklaması, https://cbddo.gov.tr/projeler/acik-veri/, Son Erişim Tarihi: 03.06.2020

[114] Open Data Barometer, https://www.opendatabarometer.org/, Son Erişim Tarihi: 03.06.2020

[115] Yılmaz, Sait ve İbrahim GÜL , 2017, "Public Security and Psychology: Changing Security Culture and Criminal Profile", Journal of Current Researches on Social Sciences, Cilt:7, Sayı: 1, Sayfa: 227-242

Bölüm 4

BİYOLOJİK BİYOMETRİK SİSTEMLER, BİYOMETRİK VERİLER, HUKUK VE GÜVENLİK

Pelin Özkaya - Refik Samet

Bilgi çağına geçişle birlikte, artık birçok işlem elektronik ortamlarda yürütülmekte ve bu işlemler neticesinde elde edilen verilerin güvenliği ve korunması en temel konu hâline gelmektedir. Bu verilere izinsiz veya yetkisiz erişimin engellenmesi ve gizliliklerinin sağlanması (gizlilik ilkesi); verilerin yetkisiz kişiler tarafından değiştirilmemesi (bütünlük ilkesi); ve verilerin yetkili kişilerce ihtiyaç duyulduğunda ulaşılabilir ve kullanılabilir durumda olması (erişilebilirlik ilkesi) adı verilen "Bilgi Güvenliği İlkeleri" (CIA Triad) göz önüne alındığında, bu ilkelere uyumun sağlanmasındaki ideal yöntemlerden birinin, kişilerin kimliklerinin tanımlanması ve doğrulanması olduğunu söylemek mümkündür. Kimlik tanımlama ve doğrulamada uygulanan yöntem ise Biyometrik Sistemler olmaktadır. Biyometri, kelime kökleri itibariyle "yaşamın ölçülmesi" anlamına gelmektedir. Yaşamın ölçülmesinden kasıt, insanın var olan özelliklerinden üretilen benzersiz biyolojik verilerin, kişinin kimliğini tanımada ve onaylamada kullanılmasıdır. Kişinin sahip olduğu bu özelliklerin değiştirilememesi ve kendine özgü olması, diğer kişilerden ayırt edilmesini kolaylaştırmakta, bu da biyometrik teknolojilerin hayatımıza girmesine vesile olmaktadır. Biyometrik sistemler, temel olarak Biyolojik ve Davranışsal olarak ikiye ayrılmakta olup, Biyolojik Biyometrik Sistemler; parmak izi, yüz, iris, retina, DNA, el geometrisi ve avuç içi tanıma gibi biyolojik özellikleri analiz eden teknolojilerle tanımlanırken, Davranışsal Biyometrik Sistemler; klavye tuş vuruşu, fare dinamiği, dudak hareketleri, göz kırpma, yürüyüş, el yazısı-imza, ses tanıma, araba sürüşü gibi davranışsal özellikleri analiz eden teknolojilerden oluşmaktadır. Bazı kaynaklar Biyolojik Biyometrik Sistemlere kılcal damar ve toplardamar yapısını da katmaktayken, bazıları kalp

ritmi, vücut ısısı, vücut kokusu, yüz ısısı gibi biyokimyasal özelikleri tanımlayan üçüncü bir sınıflandırma metodu kullanmaktadır. Bu bölümde, kimlik tanımlama ve doğrulama alanında biyometrik teknolojilerin birinci basamağı olan Biyolojik Biyometrik Sistemlerin özellikleri, bu sistemlede kullanılan teknolojilerin çeşitleri, bu sistemlerin güvenlik amacıyla kullanım yöntemleri ve biyometrik sistemlerden elde edilen özel nitelikli kişisel veri kapsamındaki Biyometrik Verilerle ilgili kanuni düzenlemeler hakkında bilgi verilmekte ve değerlendirmeler yapılmaktadır.

4.1. GİRİŞ

Biyometrik teknolojiler aslında insan uygarlığının başlangıcından beri kullanılmaktadır. İster bir öğrencinin öğretmeni tarafından tanınan ayırt edici yüz özelliği olsun, ister paranın banka hesabından çekilmesine izin veren bir çek veya Facebook'ta arkadaşlarınızın sizi bulmasına yardımcı olan profil fotoğrafınız olsun, biyometri günlük yaşamın bir parçasıdır ve olmaya devam edecektir [1].

İlk zamanlarda mekânların kapılarını kilitleyen anahtarlarla başlayan güvenlik ihtiyacı, teknolojinin gelişmesi ile birlikte, yerini yavaş yavaş elektronik teknolojilere bırakmıştır. Özellikle telefonlarda kullanılan PIN kodu, internet sitelerinde kullanıcı adı ve şifre ile giriş yapılan platformlar, hatta şifre unutulduğunda kullanılan ek kimlik doğrulama yöntemleri, şimdilerde biyometrik tanıma sistemleriyle yoluna devam etmekte. Artık çok sayıda şirketin güvenliğinin emanet edildiği bu teknolojiler en güvenli sistemler olarak kabul edilse de, siber saldırıların hedefi olmaktan doğal olarak kurtulamamakta ve çok sayıda saldırıya maruz kalmaktadır. En genel tanımı ile biyometri; sistemlere, cihazlara veya verilere erişim vermek üzere bir kişinin gerçekten 'kim' olduğunu dijital olarak tanımlamak için kullanılan biyolojik veya davranışsal insan özellikleridir. Kişiden alınan kendine özgü ve eşsiz olarak kabul edilen bu özellikler, bir donanım tarafından toplanmakta ve okunmakta, toplanan verilerin işlenmesi ve eşleştirilmesi ise yazılım tarafından gerçekleştirilmektedir.

Biyometrik teknolojilerin tarihine bakıldığında, 1970'lerde el geometrisi sistemleri geliştirilmiş ve yayılmışken; retina ve imza doğrulama sistemleri 1980'lerde ortaya çıkmış, bunu yüz tanıma sistemleri takip etmiştir. İris tanımlama ise 1990'larda kullanılmaya başlanmıştır [2].

Biyometrik teknolojilerin işleyişini en genel tanımıyla yapmak gerekirse;

- Kişiden bir biyometrik veri alınarak kaydedilir,
- Kayıtlı bu veri dijital bir koda çevrilir,
- Yapılan işleme göre şifrelenir ve veri tabanına kaydedilir,
- Kullanıcı, biyometrik verisini kayıtlı olan herhangi bir cihaza tanıtır,
- Sistem, bu kişinin gerçekten girilen kimliğin sahibi olup olmadığını, veri tabanındaki kayıtlardan aratır,
- Eşleşme sağlandığı takdirde kişi kimliğini ispatlar.

Kullanılan kimlik doğrulama yöntemlerinde, karmaşıklık ve farklı kombinasyonlar arttıkça gizliliğin ve güvenliğin de paralel şekilde arttığı bir gerçektir. Mevcut şartlar altında, parmak izi-retina, ses tanıma-iris tarama gibi çift faktörlü biyometrik kimlik doğrulama yöntemleri en güvenilir yöntemler olarak kabul edilmektedir. Zira kaybetme, unutma, unutmamak için bir yere kaydetme, her hesapta farklı şifre kullanma durumunu ortadan kaldırdığı gibi, ele geçirilme, kopyalanma veya taklit edilme olasılıkları da neredeyse imkânsızdır.

Biyometrik şifrelerde kullanmak için Uluslararası Bilgi Teknolojileri Standartları Komitesi (INCITS – International Committee for Information Technology Standards) tarafından oluşturulmuş uluslararası standartlar mevcuttur. INCITS, Amerikan Ulusal Standartlar Enstitüsü (ANSI – American National Standards Institute) tarafından onaylanan kurallara göre akredite edilmiştir ve faaliyet göstermektedir [3].

INCITS standartlarının geliştirilmesi faaliyeti aşağıdaki alanlara odaklanmaktadır [3]:

- Kimlik Kartları ve İlgili Aygıtlar
- Optik Dijital Veri Diskleri
- Siber Güvenlik
- Veri Tabanı
- Bilgisayar Grafiği ve Görüntü İşleme
- Programlama Dilleri
- Coğrafi Bilgi Sistemleri (GIS)
- Karakter Kümeleri ve Uluslararasılaşma

- JPEG ve MPEG
- Meta Veri
- Biyometrik
- Ofis Donanımı
- Açık Dağıtık İşlem (ODP)
- Radyo Frekansı Tanımlama (RFID)
- SCSI Depolama Arabirimleri
- Fiber Kanal Arabirimleri
- ATA Depolama Arabirimi
- Gerçek Zamanlı Yer Belirleme Sistemleri
- Metin İşleme
- BT Erişim Arabirimleri ve
- Öğrenme, Eğitim ve Öğretim için BT'dir.

INCITS ve ANSI biyometri ile ilgili genel standartlar oluşturduğu gibi, veri değişimi ile ilgili, yargı ve toplum kuralları için ticari uygulamalarla ilgili, havaalanında çalışanlar için fiziksel erişim kontrolüyle ilgili, sınır yönetimi, savunma, finansal endüstri ve işletmeler ile ilgili konularda da alt standartlar oluşturmuştur.

Uluslararası Standartlar Teşkilâtı (ISO - International Organization for Standardization) açısından ise, ISO/IEC JTC 1 Bilgi Teknolojisi başlığı altında; SC17 biyometrik teknolojileri kartlara ve kişisel tanımlamalara uygulamak için, SC27 biyometrik veri koruma teknikleri, biyometrik güvenlik testi ve değerlendirme metodolojileri için ve SC37 genel biyometrik standartlar için (biyometrik uygulama programlama arayüzleri, biyometrik veri değişim formatları, ilgili biyometrik profiller, değerlendirme kriterlerinin biyometrik teknolojilere uygulanması, performans testi ve raporlaması için metodolojiler ve çapraz yargı ve toplumsal boyutlar) prosedürler hazırlanmıştır [4]. Yine ISO tarafından hazırlanan ISO/IEC 27001 Bilgi Güvenliği Yönetimi standartları da daha geniş bir alana yayılan kurallar içermektedir.

ISO tarafından yapılan tanımlara göre; Standart; imalatta, anlayışta, ölçme ve deneyde bir örneklik sağlama işlemi veya standardizasyon çalışması sonucu ortaya çıkan belge ya da eserdir. Standardizasyon ise; belirli bir faaliyetle

ilgili olarak ekonomik fayda sağlamak üzere, bütün ilgili tarafların yardım ve iş birliği ile belirli kurallar koyma ve bu kuralları uygulama işlemidir. Bu standartlar uluslararası ve kıtalararası platformda üretim ve işlem yapan her uygulayıcı için uyulması gereken kurallar olması bakımından önemlidir. Gerek veri güvenliği, gerekse suçla mücadele için sınırların ötesini aşan teknoloji açısından, uygulayıcılarına senkronize hareket etme imkânını bu kurallar aracılığıyla daha kolay verebilecektir.

Bu bölümün ilerleyen alt bölümlerinde, yukarıda bahsedilen standartlar çerçevesinde, üretilmesi tavsiye edilen biyometrik teknolojiler bahsedilmekte, Biyolojik Biyometrik Sistemlerden parmak izi, yüz tanıma, iris tanıma, retina tanıma, DNA kimlik teknolojisi, el geometrisi ve avuç içi tanıma sistemlerinin özellikleri açıklanmakta, avantaj ve dezavantajlarından bahsedilmekte, bu sistemlerin karşılaştırılması yapılmakta, kamu güvenliği, sivil kimlik ve özel veri güvenliği açısından elde edilen biyometrik verilerin hassasiyeti irdelenmekte ve korsanlık faaliyetleri ile hangi hukuksal düzenlemelerin bulunduğu, örnekleriyle aktarılmaktadır.

4.2. BİYOLOJİK BİYOMETRİK SİSTEM ÇEŞİTLERİ

Biyolojik Biyometrik Sistemler, öğrenilmiş bir davranıştan ziyade, öncelikle bireyin anatomisine veya ayrıntılı fizyolojisine dayanan, otomatik tanıma için kullanılabilen, ölçülebilir biyometrik bir özelliği temel almaktadır. En bilinen Biyolojik Biyometrik Sistemler şunlardır:

- Parmak İzi
- Yüz Tanıma
- İris Tanıma
- Retina Tanıma
- DNA Kimlik Teknolojisi
- El Geometrisi
- Avuç İçi Tanıma

Her biyometrik sistemin avantaj ve dezavantajları olmakla birlikte, hangi sistemin tercih edileceği, kullanım alanına, güvenilirlik ihtiyacına, sağlamlık ve hata oranına, kullanım kolaylığı ve elbette maliyet gibi birden fazla etkene bağlı olarak farklılık göstermektedir.

4.2.1. Parmak İzi

Parmak izi analizi kimlik tespiti, tarihi çok eskilere giden ve güvenilirliği sebebiyle hâlâ kullanılan en temel sistemdir. Fiziksel parmak izi tespiti suçla mücadelede zanlının teşhisinde kullanılırken, dijital parmak izi analizi, elektronik platformlar vasıtasıyla kimlik tespitinde en çok kullanılan yöntemlerin başında gelmektedir.

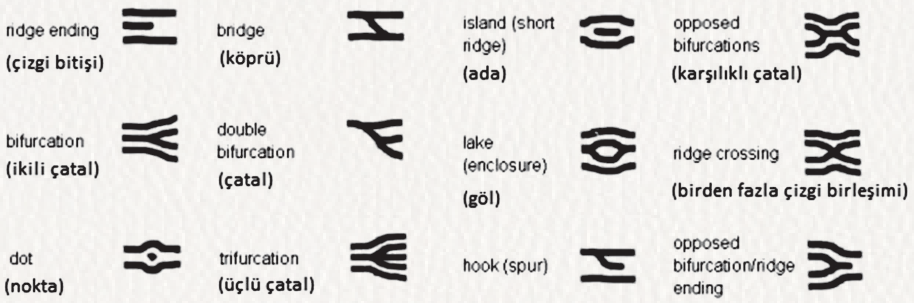
Parmak izi analizinin tarihsel geçmişine bakıldığında, M.Ö. 246 yılında Çinli yetkililer parmak izlerini belgeleri mühürlemek için kullanılan kil mühürlere vuruyorlar, Çinli tüccarlar kredileri doğrulamak için ipek veya kâğıt üzerinde parmak izlerini kullanıyorlardı. Sonraki süreçte, 1684'teki "Londra Kraliyet Cemiyeti'nin Felsefi İşlemleri" makalesinde Dr. Nehemiah Grew, parmakları ve avuç içlerini kaplayan cildin sırt yapısını tanımlayan ilk bilimsel makaleyi yayınladı [5]. Modern parmak izi kullanımı ise Sir William Herschel ile başladı, Hindistan'da 1858'den itibaren yasal belgeleri doğrulamak için parmak izleri kullanıldı. 1880 civarında Tokyo'da çalışan Dr. Henry Faulds, parmak izleri ile ilgili bir sınıflandırma metodu oluşturdu ve sınıfları çizgilerin şekline göre Yay (arch), Döngü (loop) ve Helezon (whorl) olarak ayırdı. Şekil 4.1'de gösterilen bu sınıflandırma Londra'daki Büyükşehir Polisince reddedilince Faulds, Charles Darwin'e yazdı. Darwin, bu konuda çalışamayacak kadar hasta ve yaşlı olması sebebiyle onu kuzeni Sir Francis Galton'a yönlendirdi. Galton, parmak izi analizinin mucidiydi, her parmak izinin kişiye özgü ve diğer parmak izlerinden farklı olduğunu ve kalıtıma bağlı olmadığını kanıtladı. Adli bilim olarak parmak izi analizini inceledi ve ceza davalarında kullanımları için zemin hazırladı. 1892'de "Fingerprints" kitabını yayınlayarak adli bilimlerde kullanılmasını teşvik etti. Bir katili tanımlamak için ilk parmak izi kullanımı 1892'de Arjantin'de gerçekleşti. Scotland Yard'ın Parmak İzi Bürosu 1901 yılında kuruldu [6]. 1903'te New York Eyalet Hapishaneleri parmak izlerini kullanmayı kabul etti, bunu FBI izledi [7]. 1908'de ilk resmî parmak izi kartı geliştirildi. 1911'de parmak izleri önce ABD mahkemeleri tarafından güvenilir bir kimlik belgesi olarak kabul edildi, 21 Aralık 1911 tarihinde ise, Illinois Eyalet Yüksek Mahkemesi parmak izlerinin güvenilir bir tanımlama şekli olduğu ve parmak izi kanıtlarının kabul edilebileceği sonucuna vardı [8]. 1980'ler ilk

elektronik parmak izi eşleştirme sistemini kuran bir otomasyonun yolunu açtı. "Otomatik Parmak İzi Tanımlama Sistemleri" (AFIS – Automated Fingerprint Identification System) adı verilen bu sistem, nihayetinde dünyanın dört bir yanındaki kolluk kuvvetlerinin milyarlarca parmak izi kaydını kontrol etmesini sağladı [7].

Şekil 4.1. Henry Faulds'un Temel Sınıflandırma Modeli [9]

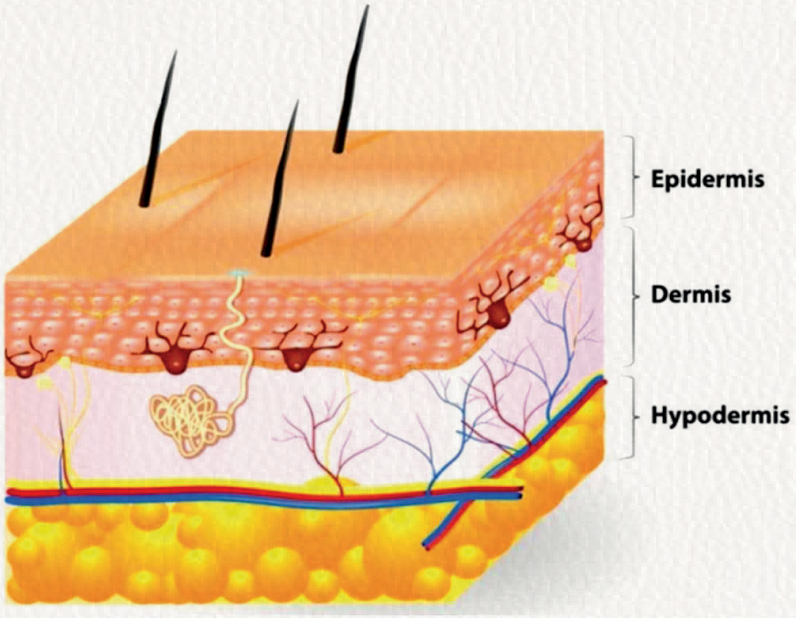
Parmak yüzeyi, sırtlardan (üst deri tabakası-çıkıntılar) ve vadilerden (alt deri tabakası-girintiler) oluşmuş olup, parmak izini kişiye özgü yapan, sırtların yani kabarıklıkların şekilleridir. Bu şekillerin her birinin farklı isimleri vardır ve parmak yüzeyindeki konumlarına göre kişiyi eşsiz ve tanımlanabilir yapmaktadır (Şekil 4.2 ve 4.3).

Şekil 4.2. Parmak İzi Sırtlarının Özelliklerine Göre İsimlendirilmesi



Şekil 4.3. Parmak İzi Alt Sınıflandırması [9]

Parmaktaki deri katmanlarında sırtlar ve vadiler, dermis ve epidermis olarak adlandırılan deri tabakalarının üzerinde bulunmaktadır (Şekil 4.4). Parmak izleri, genel olarak epidermis tabakasının bıraktığı izler üzerinden değerlendirilir ancak dermis ve epidermiste bulunan izler birbirinin aynısı olduğu için post mortem bulguların değerlendirilmesinde dermis tabakasının kullanılması fayda sağlamaktadır [10].



Şekil 4.4. Deri Yapısı

Parmak izinden gerekli özellikleri elde etmek için aşağıdaki görüntü işleme teknikleri kullanılmaktadır:

- Görüntünün gürültülerden temizlenmesi,
- Kenarların tespiti,
- Özelliklerin çıkarılması.

Parmak izinin gürültülerden temizlenmesi için Median, Mean ve Gaussian gibi filtreler, kenar tespiti için ise; Sobel, Gradient, Prewitt gibi filtreler kullanılmaktadır. Özelliklerin tespit edilmesi için kenar algılama işleminin sonucunda oluşan görüntüde, inceltme algoritmaları vasıtasıyla parmak izi çizgileri uygun hâle getirilerek, çizgilerin bitiş ve çatal noktaları elde edilmektedir [11].

Piyasada kullanılan değişik teknolojilere sahip parmak izi tanıma donanımları mevcuttur. Bunların en yaygın olarak kullanılanları Optik, Kapasitif, Ultrasonik ve Termal olarak sayılabilir:

- Optik Tarayıcılarda; parmak bir cam plakaya bastırıldığında tarayıcı, parmağın çıkıntılarını aydınlatmak için ekrana ışık gönderir. Optik sensör, parmak izinin 2D görüntüsünü yakalar ve bir CCD (Charge Couple Device) kamera parmak izinin fotoğrafını çeker. Daha fazla yansıyan ışığı temsil eden daha koyu alanlar (parmağın sırtları) ve daha az yansıyan ışığı temsil eden daha açık alanlar (sırtlar arasındaki vadiler) ile birlikte CCD sistemi, aslında parmağın ters çevrilmiş bir görüntüsünü oluşturur [12]. Optik tarayıcıların en büyük dezavantajı kandırılmasının kolay olmasıdır. Teknoloji sadece 2D bir görüntü çektiği için, protezler ve hatta yeterince iyi kalitede başka görüntülerle bu teknoloji kandırılabilmektedir [13].
- Kapasitif Tarayıcılar; baskı kullanarak ışığı algılamak yerine, kapasitörler aracılığıyla elektrik akımı kullanarak parmak izini oluşturan sırt ve vadilerin bir görüntüsünü yakalar. Kapasitif sensörler, baskının görüntüsünü yakalamak için parmak izinin yüksek ve alçak kısımları arasındaki mesafeyi kullanır, epidermal seviyesini ölçer. Kondansatörler elektrik yükünü depolayabildiğinden, bunları tarayıcının yüzeyindeki iletken plakalara bağlamak, parmak izinin ayrıntılarını izlemek için kullanılmalarını sağlar. Optik bir tarayıcıya göre kandırılması çok daha zordur. Sonuçlar bir görüntü ile çoğaltılamaz ve bir çeşit protezle kandırmak inanılmaz derecede zordur, çünkü kapasitör

üzerindeki yükte oluşan her değişiklik kaydedilir. Tek gerçek güvenlik riski, donanım veya yazılım korsanlığından kaynaklanabilir [13].

- Ultrasonik Tarayıcıda ise; çok yüksek frekanslı ses dalgaları, kullanıcının parmak izinin ayrıntılarını haritalamak için kullanılır. Kullanıcının cihazdaki kimliğini doğrulamak için hafif bir parmak dokunuşu yeterlidir [14]. Tarayıcıdaki farklı noktalarda geri dönen ultrasonik darbenin yoğunluğunu hesaplamak için bir sensör kullanılır. Daha uzun süreler boyunca tarama yapılması, taranan parmak izinin son derece ayrıntılı bir 3D modelinin çoğaltılmasına neden olur [13], bu sebeple optik tarayıcılardan daha hassas ve daha güvenlidir. Diğer tarayıcılardan farklı olarak, ultrasonik tarayıcılar, güneş kremli, ıslak veya yağlı parmakla bile çalışmaktadır [14]. Ancak bu teknoloji, çoğu erişim kontrolü uygulaması için yavaş, pahalı ve hantal olup, fazla veri yoğunluğuna sahiptir [15].
- Termal Tarayıcılarda; bir parmak sensöre konulduğunda, parmak izi çıkıntıları sensör yüzeyi ile temas eder ve temas sıcaklığı ölçülür, vadiler ise temas etmediğinden ölçülmez. Sırtlar için cilt sıcaklığı ile vadiler için ortam sıcaklığı ölçüsü tarafından bir parmak izi görüntüsü oluşturulur. Bu tekniğin en büyük dezavantajı, sıcaklık değişiminin dinamik olması ve sensör yüzeyinin sırtlara ve vadilere temas eden parmak izi görüntüsünü silerek, aynı sıcaklığa gelmesinin sadece saniyenin onda biri sürmesidir [15]. Ayrıca, bu teknoloji diğer sensörlerle aynı kirlenme ve aşınma sorunlarının çoğuna sahiptir. Geniş bir sıcaklık aralığında çalışabilirken, ortam sıcaklığı parmak yüzey sıcaklığına yakınsa, sensör en az 1 santigrat derece sıcaklık farkı oluşturmak için ısıtmaya ihtiyaç duyar [15].

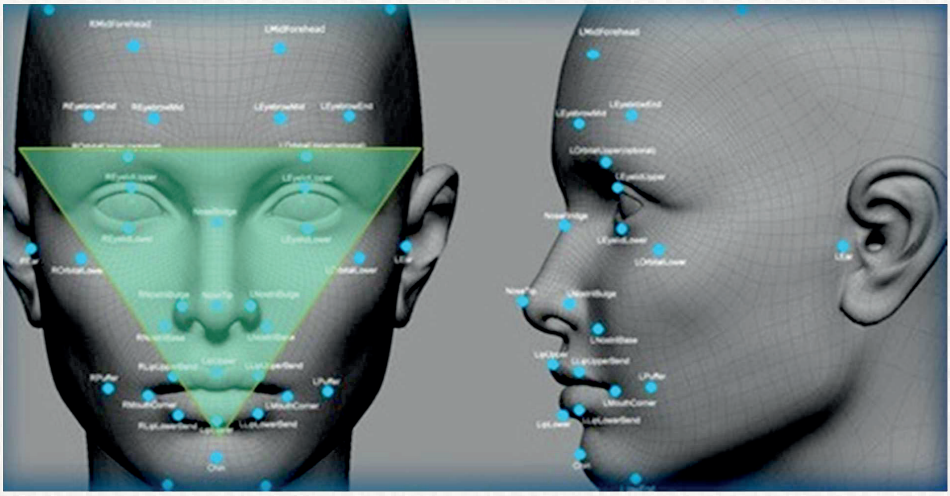
Parmak izi, ikizlerde bile farklılık gösterdiği ve kolaylıkla alınabildiği için kimlik doğrulamada en çok kullanılan yöntemdir. Bir kişinin parmak izi kolaylıkla değiştirilemediği için ve başka birisinin parmak izine benzetilemediği için de güvenilir olarak kabul edilmektedir. Bununla birlikte, eğer kişinin parmak izi kalıcı bir hasar almışsa (yanma, deri hastalıkları vb.) aynı izin tekrar elde edilmesi çok zordur. Kişinin kilo alıp vermesi gibi fiziksel değişimler parmak izinde değişikliğe sebep olabilmektedir ve eğer parmak izinin bir kalıbı varsa, bunun kendisi yerine başkası tarafından kullanılabilme sakıncası vardır. Parmak izi taklit problemi, parmak izinin alındığı parmağın

canlılığını test edecek gelişmiş sensörlerin kullanılması ile giderilebilecekken, parmak izinin hiç bulunmaması probleminin çözümü bulunmadığından bu sistem bu tip kişilerde uygulanamaz [16].

4.2.2. Yüz Tanıma

İnsanların eski zamanlardan beri birbirlerini tanımak ve kimliklerini tespit etmek için kullandıkları en eski ve en basit yöntem yüz analizidir. Yüzde bulunan burun, çene, dudak, kaşlar, gözler, kulaklar ve bunların boyutları ile aralarındaki uzaklıklar, kişileri birbirinden ayırt etmede kullanılan temel kıstaslar olmaktadır. Diğer taraftan yüzde bulunan çizgiler ve yüzün kemik yapısı da analizde faydalanılan özelliklerdendir.

Temelde yüz tanıma, bir bilgisayar yazılımı vasıtası ile yüzdeki girintiler ve çıkıntılar taranarak yapılmaktadır. Bunun için kişinin fiziki olarak orada bulunmasına gerek yoktur, video görüntüsü veya fotoğraf kullanılarak da yapılabilir. Yüzü ayırt etmeye yarayan girinti ve çıkıntılara "düğüm noktaları" adı verilmiştir ve başarılı bir yüz analizi için yazılımın 15-20 noktaya ihtiyaç duyduğu belirtilmektedir. Bu noktaların beklenen konumu, köşeleri şakaklarda ve dudak altında olan ters bir üçgen içinde kalan tüm noktalar olacaktır. Bu bölgenin, kişinin kilo alıp vermesiyle veya yaşlanmasıyla bile değişmediği kabul edilir (Şekil 4.5).



Şekil 4.5. Yüz Analizinde Kullanılan Düğüm Noktaları [17]

Yazılım tarafından ölçülen bu noktaların bazıları:

- Burnun darlığı veya genişliği
- Göz bebekleri arası mesafe
- Göz çukurunun derinliği
- Yüz uzunluğuna göre burnun üst dudakla, çenenin alt dudakla olan mesafesi
- Elmacık kemiklerinin şekli
- Yüz şekline göre gözlerin pozisyonu
- Çene kemiğinin uzunluğu
- Kulakların yüzdeki konumları

Yüz analizi yapılabilmesi için yüzün tam karşıdan açılı görüntüsü gerekmektedir. Örneğin; güvenlik kamerası veya MOBESE'ye takılan görüntülerden, suçlu analizi yapılabilmesi için yüzde gerekli noktaların tespit edilmesi gerekir, bu yüzden de "FaceDetection" adı verilen yüz bulma algoritmaları kullanılmaktadır.

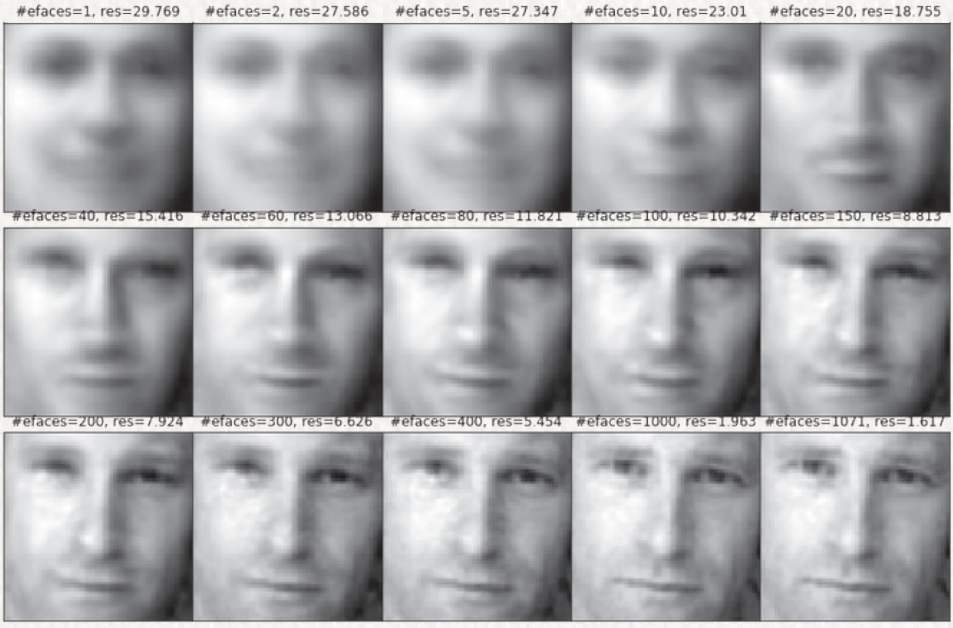
Düğüm noktaları rakamsal bir değerle kodlanır ve bu kodlara "Faceprint" denir [18]. Bu değerler yüz tanımlama yazılımının veri tabanında saklanır. Yüzdeki eğriler milimetrenin altında bir hassasiyetle ölçülerek yüzün şablonu çıkarılır. Sistem elde edilen yüz şablonunu eşsiz bir koda dönüştürür. Bu kod her bir şablonu numaralandırmış olur. Doğrulama aşamasında görüntü, veri tabanındaki sadece bir görüntüyle eşleştirilmelidir [18].

İnsan yüzünde fazla sayıda özelliğin olması nedeniyle, bu özellikleri kullanan çeşitli yüz tanıma yöntemleri (Eigenfaces, Fisherfaces, Hidden Markov Models, Evolutionary Pursuit vb.) vardır [19]:

- Eigenfaces (önyüz) Yönteminde; analizi yapılacak insanların tüm yüz görüntüleri alınır, bu görüntüler, verimli bir şekilde birlikte karşılaştırılabilecekleri bir alana yansıtılır (Şekil 4.6 ve 4.7). Eigenfaces algoritması, bir bireyi diğerinden ayıran özelliklere dikkat etmez, sadece tüm insanların tüm yüzlerini temsil eden özelliklere odaklanır. Aydınlatma önemli bir faktör olarak kabul edilir. Sistemden beklenen, aynı kişinin görüntüleri arasındaki mesafelerin, farklı insanların görüntüleri arasındaki mesafeden daha küçük olmasıdır. Eigenfaces algoritması tarafından kullanılan daha düşük boyutlu alan, aslında "Temel Bileşen Analizi (PCA - Principal

Component Analysis)" adı verilen bir süreçle öğrenilir ancak bazen bunun *"Ayrı Karhunen-Loève Dönüşümü"* olarak da adlandırıldığı görülür. Eigenfaces'in çalışma şekli nedeniyle, kullanılan yüz görüntülerinin tümü aynı boyutta olmalı ve hizalanmalıdır (tipik olarak her öznenin gözleri aynı piksel konumlarında olmalıdır) [20].

Şekil 4.6. Orijinal Yüz Görüntüsü [21]



Şekil 4.7. Özyüzler Alanına Yansıtarak Yeniden Oluşturulan Yüz Görüntüsü [21]

- Fisherface Yöntemi; Temel Bileşen Analizi yöntemi kullanılarak yüzün alan boyutunun küçültülmesine dayanır, ardından görüntünün karakteristik özelliğini elde etmek için Fisher Doğrusal Diskriminant (FDL - Fisher's Linear Discriminant) yöntemi olarak da bilinen Lineer Diskriminant Analizi (LDA - Linear Discriminant Analysis) yöntemini kullanır [22]. Fisherfaces algoritması**,** bir bireyi diğerinden ayıran temel bileşenleri çıkarır (Şekil 4.8). Dolayısıyla, bir bireyin özellikleri başka bir kişinin özelliklerine hükmedemez. Bu yöntem, Eigenfaces yöntemi kadar açık bir şekilde aydınlatma varyasyonlarını yakalamaz, değişen aydınlatmada bile iyi sonuçlar verebilir [23].

Şekil 4.8. "Yale Yüz Veritabanı"ndaki Farklı Yüz Pozlarına Sahip Birçok Görüntü Örneği [24]

- Hidden Markov Models (HMM – Gizli Markov Modelleri); özellikle konuşma, el yazısı, jest tanıma, konuşma parçası etiketleme gibi uygulamalarıyla bilinir ve Markov zincirini güçlendirmeye dayanmaktadır. Bir Markov zinciri, her biri gruptan değerler alabilen rastgele değişkenlerin, durumların olasılıkları hakkında bilgi veren bir modeldir. Bir Markov zinciri, bir dizi gözlemlenebilir olay için bir olasılık hesaplanması ge-

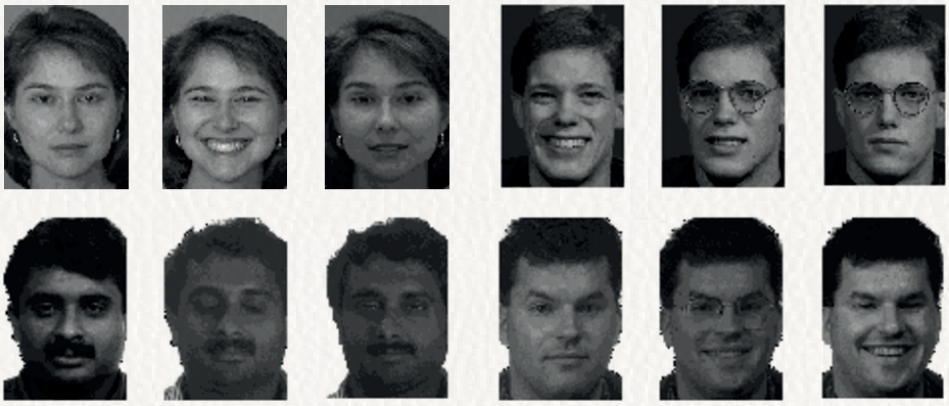
rektiğinde yararlıdır. Bununla birlikte, çoğu durumda, ilgilenilen olaylar gizlidir, doğrudan gözlemlenemez [25]. HMM yönteminin uygulanması aşağıdaki gibi özetlenebilir:

- Bir medyan filtre kullanarak yüz görüntüsünün filtrelenmesi,
- Çok sayıda ayrık dalgacık dönüşümü (DWT) kullanılarak ek gürültü ve görüntü boyutunun azaltılması,
- Bir Gauss karışım katsayısı ile sürekli çıkış yoğunluğunun tek durumlu HMM'ini kullanarak DWT'nin sonuçlarını çalışmak,
- Doğrulama için görüntüleri tanımak [26] (Şekil 4.9 ve 4.10).

Şekil 4.9. HMM Tarafından Bulunan 5 Durum İçin Çalışma Görüntüleri ve Ortalama Vektörler [27]

Şekil 4.10. Önden Görünüm Örneği, Oluşturulan ve Gerçek Profil [**27]**

- Evolutionary Pursuit (EP - Evrimsel Arayışı); genetik algoritmaları kullanarak sınıflandırma yapan bir yöntemdir (Şekil 4.11). Yüz görüntülerini daha düşük boyutlu beyazlatılmış bir PCA alt uzayında işler. Bu alt uzaydaki temel vektörlerin yönlendirilmiş ancak rastgele dönüşleri, evrimin performans doğruluğu ve sınıf ayrımı (dağılım indeksi) olarak tanımlanan bir uygunluk fonksiyonu tarafından yönlendirildiği genetik algoritmalar tarafından araştırılır [28].



Şekil 4.11. Evolutionary Pursuit Tanıma Sistemi Sınıflandırma Örneği [28]

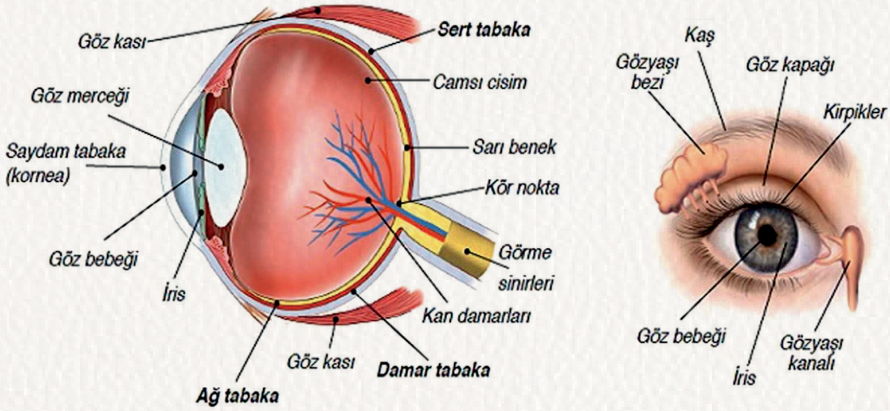
İnsan yüzü ve analizde temel alınan düğüm noktaları ele alındığında, tek yumurta ikizleri hariç, her insanın yüzünün birbirinden farklı olması ve taklit edilmesinin oldukça güç olması, bu yöntemin analizini kolaylaştırmaktadır. Yüz tanıma cihazları oldukça yüksek çözünürlüğe sahip olan cihazlardır. Bu cihazlara tanımlanacak olan kişilerin yüzünde makyaj olması veya saçının, sakalının, bıyığının vb. bulunması hiç önemli değildir. Bir kamera veya fotoğraf yardımıyla kolaylıkla yüz analizi yapmak mümkündür, bunun için kişinin fiziki olarak karşınızda olmasına gerek yoktur.

Yüzdeki herhangi bir organda eksiklik veya deformasyon, kimlik tanımada büyük kolaylık sağlayabilir. Bununla birlikte, günümüz teknolojisini düşündüğümüzde silikon bir maskeyle veya plastik makyajla yüzün taklit edilmesi sağlanabilmektedir ancak mimiklerin ve yüz çizgilerinin birebir taklit edilmesi yine de zordur. Çözünürlüğü düşük bir görüntüyü belli dereceye kadar yanıltabilmesi ise bir başka soruna teşkil edebilir veya algoritma, benzer mimiklerin aynı kişiye ait olduğuna dair yanlış kararlar verebilir.

Yüzde oluşan bir darbe veya keskin bir yara, analizi zorlaştıran faktörlerdendir. Görüntünün alındığı çevre koşulları da yanıltma sağlayabilir. Yaşa bağlı değişiklikler sebebiyle kişinin 15 yaşından büyük olması ve her 10 yıl gibi bir sürede analizin tekrarlanması önerilmektedir.

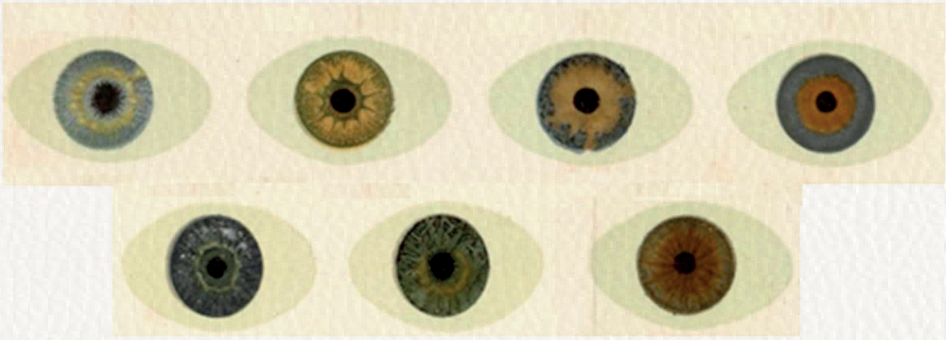
4.2.3. İris Tanıma

İris, göz bebeğinin etrafında yer alan göze rengini veren renkli halkaya verilen isimdir (Şekil 4.12) ve parmak izi gibi kişiye özeldir. Genellikle retina ile karıştırılır. İris tanımayı diğer biyometrik sistemlerden ayıran en önemli özellik ise kopyalanamaz ve taklit edilemez olmasıdır.



Şekil 4.12. İris'in Yapısı

Kişi tanımlaması için iris kullanma düşüncesini ilk olarak ortaya atan Fransız göz doktoru, antropolog ve polis memuru Alphonse Bertillon'dur [29] (Şekil 4.13) ve 150 yıldan fazla bir süre sonra, dünya hâlâ Bertillon'un yolundan gitmektedir.



Şekil 4.13. Farklı İris Tonlarının Tablosu, Alphonse Bertillon, 1893 Wellcome Kütüphanesi, Londra [30]

1981'de iki göz doktoru, Aran Safir ve Leonard Flom; irisin, biyometrik sistemlerde kullanılabileceğini savunmuşlardır [31]. 1989'da Cambridge Üniversitesi'nden Dr. John Daugman'ın öncülüğünde bir grupla birlikte Safir ve Flom, iris tanıma sisteminin algoritmasını geliştirerek, 1987'de bu düşüncenin patentini almışlardır [32].

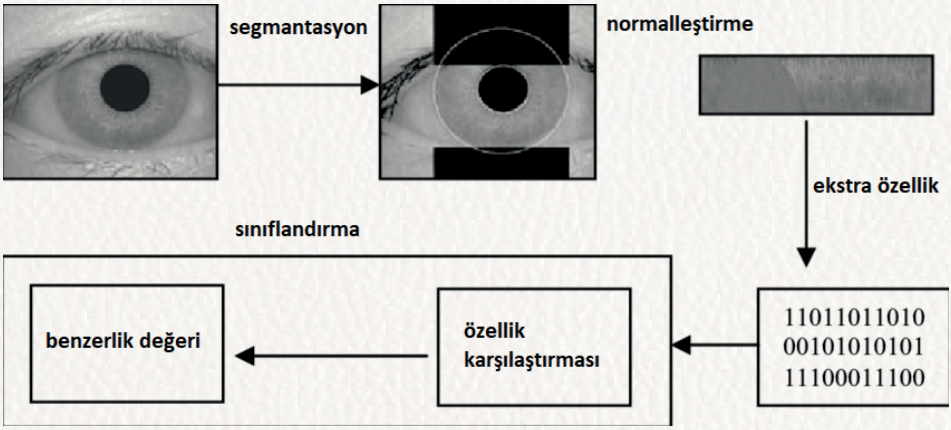
Bir iris içindeki belirli noktaları bulup tanıyan İris tarama teknolojisi, bir bireyi tanımlamanın en güvenli yollarından biri olarak kabul edilmektedir. İriste 250'den fazla görsel karakteristik bulunmaktadır. Bunlar daireler, benekler, çizgiler gibi belirleyici şekillerdir [33].

İris tanıma teknolojilerinin kimlik tespitinde tercih edilmesinin çok sayıda nedeni vardır [31]:

- Kişinin gözlüklü veya lensli olması iris analizini etkilemediği gibi, göz rengi de belirleyici bir faktör değildir,
- İris, sol ve sağ göz arasında farklı olduğundan, tanıma her göz için ayrı ayrı yapılabilir,
- Kişi kendini tanıtmak için sabit ve yakın durmak zorunda değildir, hareket hâlindeki ya da 1-2 metre uzaklıktaki kullanıcıları bile kolay ve hızlı şekilde tespit edebilir,
- İris, kopyalanamaması sebebiyle çok düşük hata oranına sahip olup, güvenilirliği fazladır,
- Kızılötesi kamera kullanıldığından sistem gece saatlerinde veya karanlıkta bile kullanılabilir,
- Dünyada aynı irisin bulunma olasılığı $1/10^{78}$'dir, dolayısıyla iris eşsiz kabul edilmektedir, tek yumurta ikizleri de buna dâhildir,
- Kalıtımsal hastalıklardan etkilenmezken, genetik oluşumlardan çok az etkilenmesi değişmezliğini ve güvenirliğini arttırır,
- İris anne karnında embriyo iken oluşur ve ölüme kadar değişmeyen tek organ olarak kabul edilir. Ölümün ardından 3 sn sonra canlılığını yitirmesi de aslında güvenilirlik için önemli özelliklerden biridir.

İris tanıma, genellikle hız ve doğruluk isteyen yüksek teknolojili ortamlar için ideal olan fiziksel erişim kontrol yöntemi olarak kullanılır. Yüz ve ses tanıma

gibi yazılım tabanlı değil, donanım tabanlıdır. Yüksek teknolojili ve pahalı kameralar kullanılması sebebiyle de tüketiciye yönelik dağıtımları daha azdır. Ayrıca kara, deniz ve hava yoluyla ülkelere girip çıkarken yolcuları tanımlayabilen sınır kontrol uygulamalarında, güvenli havacılık sistemlerinde, hastanelerde ve tesislere giriş çıkışlarda yetkili erişim için vb. sıklıkla kullanılmaktadır. Winthrop Üniversitesi'nin EagleEye katılım izleme sisteminde ve İsviçre'nin Cenevre kentindeki Büyük Hadron Çarpıştırıcısı ile ünlü CERN'de İris teknolojisi kullanılmaktadır [33].



Şekil 4.14. İris Tanımanın Temel Aşamaları [34]

İris Tanımanın çalışma şekli şu şekildedir [34]:

- İnsan gözündeki renkli halkaların benzersiz desenlerini ölçmek için görünmez kızılötesi ışınlar kullanır, her göze özgü olan yaklaşık 240 biyometrik özellik toplar,
- İrisin sınırlarının ve dokularının ayrıntılı bir görüntüsünü almak için kirpikleri, göz kapaklarını ve aynasal yansımaları analizden çıkarır,
- Daha sonra, iris içindeki bilgileri kodlayan bir bit deseni çıkarmak için göz çizgilerinin ve renklerinin desenini analiz eder,
- Bu bit desenini sayısallaştırır ve program bu görüntüyü bir algoritma tarafından okunacak benzersiz bir koda dönüştürür ve doğrulama (birebir şablon eşleme) veya tanımlama (bire çok şablon eşleme) için bir veri tabanında depolanan şablonlarla karşılaştırır (Şekil 4.14).

2009 yılında yapılan bir araştırma, akut iris inflamasyonu (iritis veya anterior üveit olarak da bilinir) olan hastaların, mevcut iris tanıma sistemlerinin başarısız olmasına neden olduğunu tespit etmiştir [35]. Ulusal Standartlar ve Teknoloji Enstitüsü'nün (NIST) 2012 raporu, bir kalabalığın içinde bir bireyi tanımlamak için kullanılan iris tanıma teknolojisinin %1 ila %10 oranında yanlış olduğunu göstermiştir. Ayrıca iris tarayıcılarını kandırmak veya atlatmak da mümkündür. 2012 yılında, Universidad Autonoma de Madrid'deki güvenlik araştırmacıları, güvenlik veri tabanlarında depolanan dijital kodlardan görüntüleri yeniden oluşturabildiler [36]. Almanya'daki Chaos Computer Club'a sahip bilgisayar korsanları ise, Samsung'un Galaxy S8 akıllı telefonundaki iris tabanlı kimlik doğrulamasını gece çekimlerinde, sadece yüzünün dijital bir fotoğrafını çekerek atlatabildiler [36].

Akademisyenler bazı hastalıkların iris tanıma sistemlerinin doğruluğunu bozabileceğini söylemektedir. Araştırmalar ayrıca, belirli koşullarda, kontak lenslerin iris tanıma programlarının doğruluğunu ve performansını bozabileceğini göstermiştir. Koyu renk gözlü insanlar, taramada bazı sorunlara neden olabilmektedir, bu sebeple ışıklandırma iyi yapılmalıdır. Ayrıca gözleri görmeyen kişilerin kimlik tanıması yapılamamaktadır [37].

İris tanıma için gözün doğru açısının yakalanabilmesinin zorluğu, kalite düşüklüğü, hareket ve odak bulanıklığı, görüntü işleme ve depolama sorunları, okuma mesafesinin yakın olması, ortamdaki aydınlanmadan etkilenmesi gibi konular, bu sistemlerin diğer dezavantajları olarak görülmektedir.

4.2.4. Retina Tanıma

Retina, göz yuvarlağının iç kısmında yer alan damarlarda ince sinirlerin yer aldığı ağ tabakadır. Retina taramasında kullanılan cihazlar göz bebeğinin arkasındaki kılcal damarlardan oluşan tabakanın taramasını yaparlar (Şekil 4.15). Bu kılcal damarlar retinanın eşsiz olmasını sağlayan çok karmaşık bir düzenlemeye sahiptir, dolayısıyla tek yumurta ikizleri dâhil olmak üzere, her insanın kılcal damar düzenlemesi farklı olduğundan, bu sistem kimlik tanıma teknolojilerinde yerini almıştır.

Şekil 4.15. Retina Tarama [38]

Şekil 4.16. Retina Tanıma Sistem Örneği

Retina tanımanın çalışma prensibi [39]:

- Kişi, gözünü Şekil 4.16'daki gibi bir donanım tarayıcısının göz merceğine yerleştirir,
- Düşük enerjili kızılötesi ışık, retinayı tamamen aydınlatmak için göze gönderilir,
- Retinanın kan damarları, gözün geri kalanından daha emici olması nedeniyle, bu ışığın yansıma miktarı tarama sırasında değişir,
- Esnek görüntülerin yakalandığından emin olmak için, kızılötesi ışık dönüşünü tamamlarken kişi hareketsiz durmalıdır,
- Elde edilen veri noktalarından (Retinadan 400'e kadar benzersiz veri noktası yakalanabilir) kayıt şablonu oluşturulur ve veri tabanında saklanır (retina kayıt şablonunun boyutu yalnızca 96 bayttır, en küçük biyometrik şablon olarak kabul edilir),
- Doğrulama ve kayıt şablonları arasındaki istatistiksel yakınlık incelenir.

Doğrulama ve kayıt şablonları arasındaki istatistiksel yakınlığı incelerken çok daha düşük işlem yükü gerekir. Bu küçük boyut, daha fazla sayıda şablonun tek bir veri tabanında saklanabileceği ve boyutların çok daha büyük olduğu Yüz Tanıma Şablonları veri tabanına kıyasla, çok daha verimli olacağı anlamına gelir. Sistemin bir bireyin kimliğini onaylaması için geçen süre de çok hızlıdır; iki saniyeden kısa sürede gerçekleşebilir [39].

İris gibi, retina da bir hastalık veya körlükten etkilenmedikçe bir bireyin yaşamı boyunca hemen hemen değişmeden kalır. Ancak bu kılcal damarlar, diyabet gibi göz ve damar hastalıklarından, AIDS, sıtma, suçiçeği gibi bulaşıcı hastalıklar ve lösemi, lenfoma gibi kalıtsal hastalıklardan etkilendiği için kullanışlı bir yöntem olarak kabul edilmemektedir. Hamilelik de gözleri etkilemektedir. Benzer şekilde, konjestif kalp yetmezliği, damar sertliği ve kolesterol sorunları gibi kronik sağlık durumlarının belirtilerinin ilk olarak gözlerde görüldüğü söylenmektedir.

Retina damar ağının eşsizliği ve dışarıdan müdahalesiz gözlemlenememesi, sistem güvenirliliğini yükselterek, yanlış tanıma oranını oldukça azaltmaktadır. Retinanın sahip olduğu çok sayıda benzersiz veri noktası nedeniyle, bir bireyin kimliği doğrulandığında, gerçekten o kişi olduğu hemen hemen hiçbir hataya yer bırakmaz, bir sahtekârın bir retina tanıma sistemi tarafından yanlışlıkla kabul edilmesinin istatistiksel olasılığı neredeyse yoktur [39].

Günümüzde kullanılan biyometrik sistemler arasında en pahalı ve en yüksek güvenliğe sahip olan sistem retina tanımadır. Bunun yanı sıra, tarama yapılırken gözün bir müddet hareket ettirilmemesi ve kırpılmaması gerektiğinden dolayı, çok sayıda deneme yapılması ihtimali ve doğru sonucu elde etmenin uzun zaman alması, gözün arka bölgesinin aydınlatılmasının maliyetinin yüksek olması ve lazer etkisinin hassas olan göz yapısına zarar verme tehlikesi, bu yöntemin az tercih edilmesine yol açmaktadır.

4.2.5. DNA Kimlik Teknolojisi

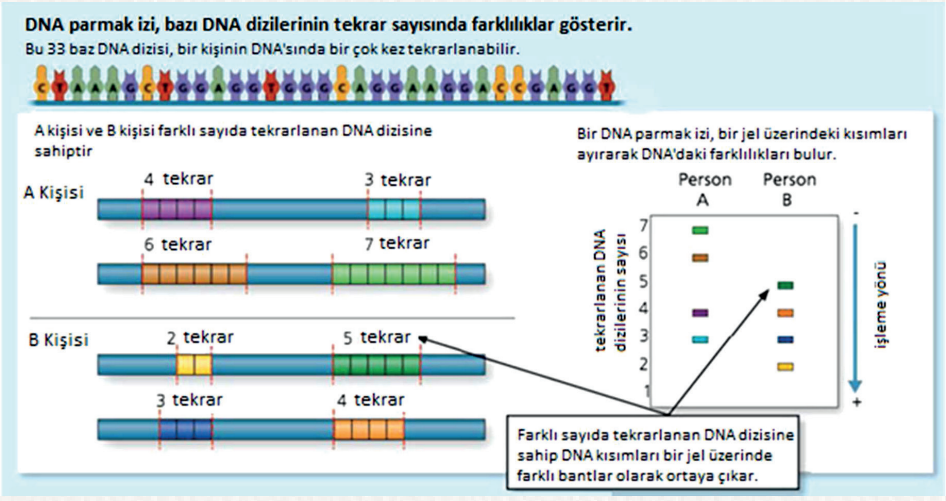
Biyometrik tanıma sistemlerinin çeşitli olası türleri arasında Deoksiribonükleik Asit (DNA), bir kişinin hayatı boyunca ve ölümünden sonra değişmez. Adenin (A), Guanin (G), Sitozin (C) ve Timin (T) nükleotid monomerleri

herkeste bulunuyor olsa da, yan yana gelerek oluşturdukları DNA zincirleri, kişilerin genotipik yapılarının farklılaşmasına neden olur. Tek yumurta ikizleri haricinde, iki insanın aynı DNA profiline sahip olma olasılığının yaklaşık olarak trilyonda birden az olduğu belirtilmektedir.

Kişinin saç, tırnak, deri, sperm, kan, tükürük vb. biyolojik materyallerinin incelenmesi sonucu, içinde bulunan DNA moleküllerindeki dizilim incelenir. Özellikle emniyet güçleri tarafından olay yeri inceleme sonucu bu alanda bulunan biyolojik materyallerin incelenmesiyle suçlulara ulaşılır. Ya da hukuki olaylarda babalık davalarının sonuçlanması işlemlerinde kullanılmaktadır. Doğruluğu çok yüksek bir yöntem olarak kabul edilmektedir, numune ne kadar ayrıntılı olursa, tanımlama da o kadar kesin olmaktadır [40].

DNA profillemenin temel adımları şunları içerir [41]:

- DNA, kan, tükürük, saç, kıl veya dokudan ayrıştırılır,
- DNA örneği, bilinen değişken sayıdaki ardışık tekrar dizilerini (VNTR) içeren daha kısa bölümlere ayrılır,
- DNA dizileri boyuta göre düzenlenir,
- Çeşitli örneklerden alınan DNA dizileri karşılaştırılır (Şekil 4.17).



Şekil 4.17. DNA Parmak İzi Analiz Şeması [41]

Çoğu zaman, DNA biyometri teknolojisi, doğrulamanın aksine tanımlama amacıyla kullanılır. Bir DNA profili oluşturma süreci olan DNA dizilimi, daha önce bir veri tabanına alınmış ve kataloglanmış DNA örnekleri ile karşılaştırılır. Mevcut en yaygın DNA veri tabanı, Federal Soruşturma Bürosu tarafından kullanılan 'CODIS Sistemi'dir. DNA biyometri teknolojisi evrensel kullanım için yeterince gelişmiş değildir, mevcut DNA biyometri, filmlerde gösterilenden çok uzaktır [42].

Doğruluğu çok yüksek bir yöntem olmasına rağmen pek çok dezavantaja da sahiptir. DNA'nın elde edileceği biyolojik dokunun kirlenmesi gibi durumlarda örnek kalitesi düşeceğinden analiz yapmak zorlaşır. 24 saat gibi bir sürede gerçekleştirilme zorunluluğu ve yüksek maliyetli olması diğer dezavantajlarıdır [25].

Bir DNA sisteminin güvenliğini sağlamak için birtakım güvenlik problemleri bulunmaktadır. Örneğin; DNA veri tabanının güvenliğini sağlamak için güvenlik mekanizmalarının uygulanması konusunda bilgi saklama süresinin ne kadar olacağı veya kimlere erişim hakkı verileceği temel sorunlardır. Benzer şekilde, sadece öncelikli amaçlar için kaydedilen bilgilerin kullanılıp kullanılmadığı ve yüksek seviyede gizlilik bulunup bulunmadığı konuları da dikkate alınması gereken mevzulardır. DNA örneğini elde etmenin fiziksel zorunluluğu ve DNA karşılaştırması yapmak için gereken zaman ile numunenin bulaşması ihtimali de kimlik tanımlamayı zorlaştıran etkenlerdendir.

California San Diego'daki Ulusal Üniversite'den Samuel Afuwape, mevcut DNA biyosensörlerini "İyon Seçici Alan Etkili Transistör (ISFET)" adı verilen yeni bir cihazla birleştirecek taşınabilir bir DNA sıralayıcı üzerinde çalışmaktadır. Bu ürün, elde taşınır bir cihazın şu anda bir laboratuvarda yapılması gereken işlemlerin aynısını yapmasına imkân verebilecektir. Bu tür gelişmeler gerçekleştikçe, fiziksel ve ağ güvenliğinde kullanılmak üzere DNA biyometrisinin sivil iş ortamlarına uygulanması büyük ölçüde genişleyecektir [43].

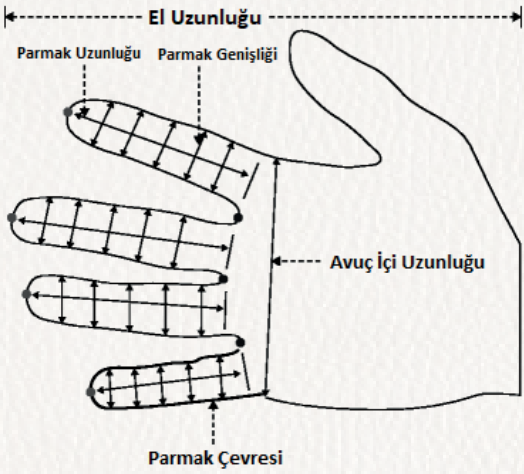
4.2.6. El Geometrisi

Herkesin el ve parmakları birbirinden farklıdır ve kendine has birtakım özellikler taşır. Fakat bu farklılık, diğer biyometrik sistemler gibi benzersiz veri noktasına sahip olması sebebiyle değil, elin şeklinden kaynaklanmaktadır. Parmak izi veya iris kadar benzersiz bir yapıya sahip olmadıklarından kimlik tanımlamadan ziyade kimlik doğrulama için kullanılmaktadır.

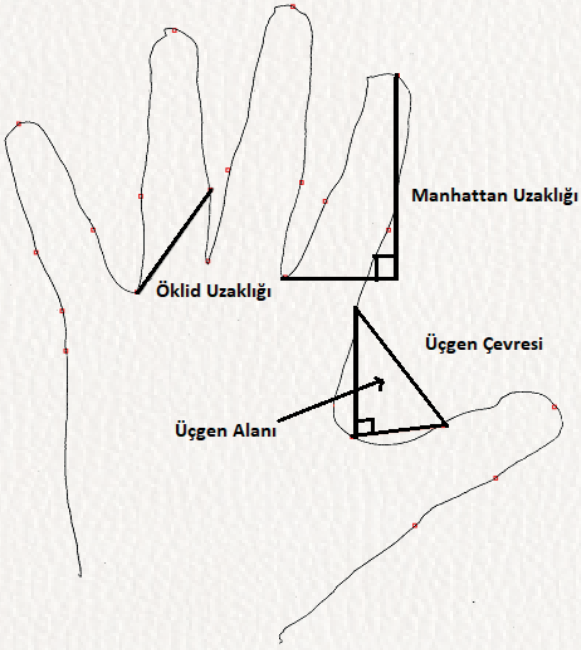
El geometrisi tanıma teknolojisi, geliştirilen ilk biyometrik tanıma sistemidir ve tüm biyometrik sistemlerin en uzun uygulama geçmişine sahip olanıdır, doğuşu 1960'lara kadar uzanır. Bilinen ilk kullanımı, Wall Street'te bulunan Shearson Hamill Bankası'ndadır. 1985 yılında David Sidlauskas el geometrisi konseptini geliştirip patentlenmiş ve ilk ticari el geometrisi tanıma sistemlerini ertesi yıl piyasaya sürmüştür. 1996 Olimpiyat Oyunları, Olimpiyat Köyü'ne fiziksel erişimi kontrol etmek için el geometrisi sistemlerini kullanmıştır [44]. Walt Disney World, parka girişini kolaylaştırmak, konukları sezonluk bilet sahipleri olarak tanımlamak ve sahtekârlığı önlemek amacıyla benzer bir "parmak" geometri teknoloji sistemi kullanmıştır [44].

Şekil 4.18. El Geometrisi Okuyucu Sistem Örneği

El geometrisi sisteminin çalışma prensibine bakıldığında, el cihazın üzerine konulur ve parmaklar ölçüm yuvasına uygun şekilde yerleştirilir (Şekil 4.18). El tarama için bir CCD (Charge Coupled Device) kamera gereklidir. Bu kamera, elin üstünden ve yanından fotoğraflarını alarak bir şablon oluşturur [40], bu bilgiler sayısal bilgiye çevrilir ve veri tabanındaki kayıtlar ile kıyaslanır. Ele ait uzunluk, elin genel şekli, kalınlık, parmakların uzunluğu, eni, büküm yerleri, eğriliği gibi bilgiler analiz edilir (Şekil 4.19.a). Elin karakteristik özelliklerini elde etmek için el ve parmakların belli noktalarına ihtiyaç duyulmaktadır; bu sınırlar, parmakların uç noktaları, vadi noktaları ve bileğin konumu olarak kabul edilmektedir [45]. El geometrisi tarayıcıları, avuç içi ayrıntılarını dikkate almamakta, parmak izleri, avuç içi yaşam çizgileri veya diğer sırtlar, renkler ve hatta el yüzeyindeki bazı yara izleri ile ilgilenmemektedir.



(a) El Geometrisi Teknolojisi

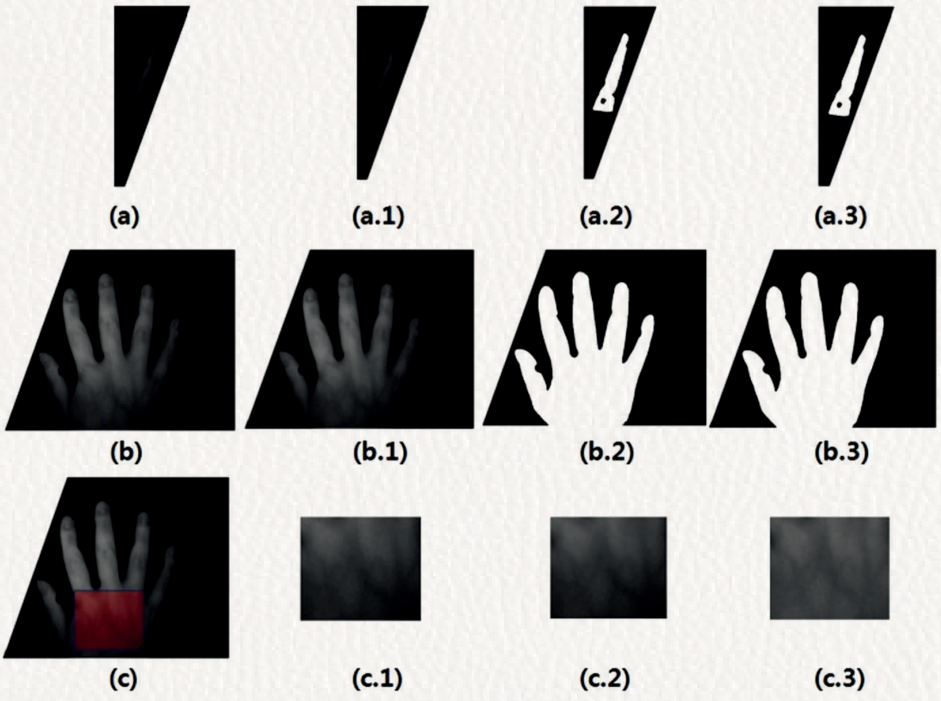


(b) El Geometrisinde Hesaplama Yöntemi

Şekil 4.19. El Geometri Teknolojisi ve Yöntemleri

El geometrik özellikleri, sağ elin dört parmağı dâhil olmak üzere, üst avuçtan çıkarılır, bunun için, başlangıçta, sağdan dört parmak ucu ve iki köşe vadi noktası tahmin edilir. Bundan sonra, bu parmak ucundan ve vadi noktalarından sekiz mesafe kenarı hesaplanır [46]. Bu sekiz mesafe kenarından üç üçgen tahmin edilmektedir (Şekil 4.19.b). Bu üç üçgen alan, üç özellik olarak kullanılır ve özellik vektörü olarak veri tabanında saklanır. Son olarak, test adayı el özelliği Öklid uzaklığı metriği üzerinden önceden tanımlanmış veri tabanı özellik vektörü ile karşılaştırılır [46]. Önerilen doğrulama sistemi 250 kullanıcı görüntüsünün kendi veri kümesi boyutu ile test edilir, yani 1250 el görüntüsü ve sonuçlar, mevcut teknolojiye kıyasla önemli bir iyileşme gösterir [46].

El taraması yapılırken, daha iyi bir analiz için zıtlık arttırılıp (Şekil 4.20), elin arka plandan daha iyi bölümlere ayrılması sağlanabilir ve sahte pikseller eşikleme kullanılarak kaldırılabilir. Görüntü elin küçük sapmalarını gidermek için yeniden boyutlandırılıp döndürülebilir. Elin formunu çıkarmak için kenar algılama algoritmaları (örneğin, ayıklamak için uygulanan Sobel) kullanılabilir [47].



Şekil 4.20. El Taraması Algoritmalarının Uygulanmış Görünümü [47]

El tanıma için el görüntüsü yakalandığında ön işleme iki adımda gerçekleştirilir [47]:

1. Gri görüntü, arka planın ortadan kaldırıldığı siyah beyaz bir görüntüye dönüştürülür. Elin yandan görünüşü için ön işleme Şekil 4.20 (a)'da, eldeki veriler için ön işleme Şekil 4.20 (b)'de gösterilmiştir.
2. Şekil 4.20 (c)'de gösterildiği gibi, vasküler örüntü çıkarma (VPE) algoritmasını başlatmak için gürültü çıkarılır. Şekil 4.20 (a.1), (b.1) ve (c.2) gürültü giderme için Gauss filtresini göstermektedir. Şekil 4.20 (a.2), (b.2) eşiği, Şekil 4.20 (a.3) ve (b.3) eşik görüntüsündeki paraziti azaltma için medyan filtresini göstermektedir. Şekil 4.20 (c.3)'te vasküler örüntüleri vurgulamak için yüksek geçirgen filtre gösterilmektedir [47].

Hem kayıt hem de doğrulama şablonlarını oluşturmanın bir kusuru vardır; elin geometrik özelliklerindeki bazı fizyolojik benzerlikleri bir diğeriyle paylaşmasıdır. Bu sorunun hafifletilmesine yardımcı olmak için, "Temel Bileşen Analizi" kullanılmaktadır. Bu, benzersiz özelliklerin ayıklanabilmesi için bir dizi ilişkisiz özelliğin ham görüntülerden "klonlanmasına" olanak tanır.

El geometrisi tanıma sisteminde, kullanıcının kimlik saptama yapılacak yerde bizzat bulunması gerektiğinden, özellikle yüksek güvenlik gerektiren cezaevi, askerî tesisler gibi yerlerde yaygın olarak kullanılmaktadır. El tanıma sisteminin diğer bazı uygulama alanları:

- Binalara, tesislere ve ofislere erişim,
- Kiralık kasalara erişim,
- Yüksek güvenlik bölgelerine erişim,
- Hastanelerde yeni doğan ünitelerine erişim,
- Okullarda öğrenci devam takip ve erişim kontrol, veli kontrolü,
- Elektronik ödeme işlemleri,
- Elektronik bilet satışı,
- Kombine bilet uygulamaları,
- Hastane ve sigorta kuruluşlarında hasta takibi ve kimlik saptama,
- Kamu hizmetlerine yönelik kayıt takibi (SSK, vergi, trafik vb.),
- Personel devam ve takip uygulamaları.

Ulusal ve uluslararası düzeyde el geometrisi teknolojisine odaklanan standart geliştirme çabaları, kimlik doğrulama tabanlı güvenlik çözümlerinin geliştirilmesini hızlandırmayı amaçlamaktadır. ANSI INCITS 396-2005 El Geometrisi Değişim Biçimi, el siluetinden toplanan el geometrisi bilgilerinin saklanması, kaydedilmesi ve iletilmesi için veri değişim biçimini tanımlamaktadır [48]. Bu ulusal standart, ISO/IEC CD (Komite Taslağı) 19794-10 Biyometrik Değişim Biçimi - Bölüm 10, Uluslararası standartlar seviyesindeki El Geometrisi Siluet Verilerine (ISO/IEC) karşılık gelmektedir [48].

El ve parmak geometrisi ile kimlik doğrulama sistemlerinin güçlü yanları olduğu gibi zayıf yanları da bulunmaktadır. Elin sakatlanması, deforme olması, parmak kaybı, gut hastalığı, kireçlenme, el boyutundaki değişiklikler, kilo alımı-kilo kaybı, elde bulunan yüzük gibi aksesuarlar ve yara bandı gibi maddeler bu sistemin yaygınlaşmasını engellemektedir. Ayrıca, elin yerleştirildiği plakanın hijyeni önemlidir, çünkü son kullanıcı tarafından doğrudan temas gerektirir. El taraması için kullanılacak cihazların, diğer biyometrik yöntemler için kullanılan cihazlara göre kaplayacağı alan daha büyüktür. Bu nedenle alan kullanımının önemli olduğu durumlarda tercih edilmemektedir [40]. Çocuklarda, el ve ayakların çok hızlı büyüdüğü hastalıklara sahip kişilerde ise bu sistem kullanılamamaktadır.

Diğer taraftan soğukluğun ve sıcaklığın yüksek olduğu hava şartlarında kullanılabilir ve hatta kasırga ve Tsunami gibi doğa olaylarına dayandığı bilinmektedir. Nüfus sayısının yüksek olduğu fabrikalarda, depolarda ve tesislerde kullanılabilir. Tek bir cihazın, farklı bireylerin 40.000'den fazla biyometrik şablonunu saklayabildiği söylenmektedir. El geometrisi tanımanın taklit edilmesi çok zordur, çünkü bu, elin 3 boyutlu bir fiziksel modelinin oluşturulmasını gerektirir.

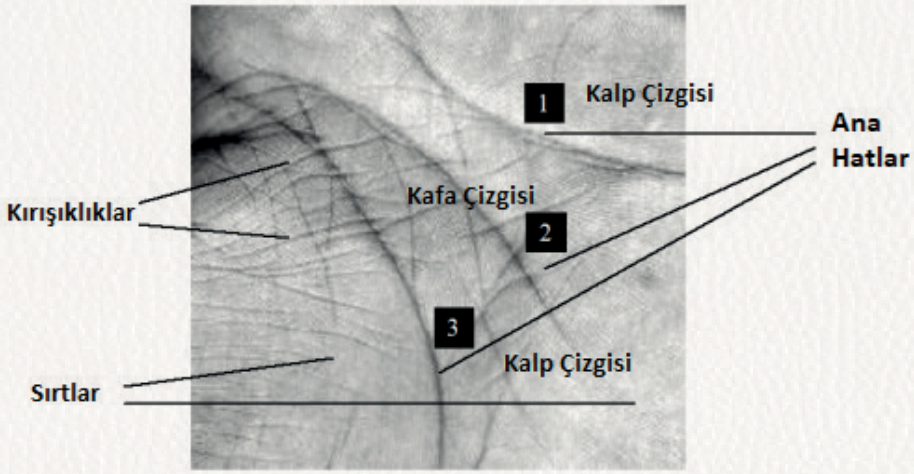
4.2.7. Avuç İçi Tanıma

Avuç içi görüntüleri, genetik ve/veya çevresel faktörlere bağlı olarak her birey için farklı şekilde oluşmuş desenlerdir [49]. Avuç içi tanıma sistemlerinde, avuç çizgilerinin özelliklerinin, konumlarının, sayılarının belirlenmesi üzerinde durulduğu gibi, avuç içi damar okuyucu özelliği olan cihazlar, avuç içi ayasındaki damar ağlarını okuyarak, örneğin damar çatallanmaları gibi ayırt edici öznitelikleri analiz etmeye yaramaktadır.

Tarih boyunca birçok durumda el yazısının incelenmesi, okuma yazma bilmeyen kişileri kendi adlarını yazamadıkları için ayırt etmenin tek yöntemiydi. Buna göre, bir isim kaydedemeyen ancak imzalanmış bir eli sözleşmenin arkasına basabilenlerin el izleri kabul edilebilir bir kimlik biçimi hâline geldi. 1858'de Hindistan Kamu Hizmeti için çalışan Sir William Herschel, çalışanlarını ayırt etmek için sözleşme arkasına el izlerini kaydetti [6]. Avuç içi baskıları desteklemek için üretilen, bilinen ilk AFIS sisteminin bir Macar şirketi tarafından yapıldığına inanılmaktadır. Avuç içi sistemine gömülü avuç içi ve parmak izi tanıma teknolojisi, daha sonra 1997'de bir ABD şirketi tarafından satın alındı. 2004 yılında Connecticut, Rhode Island ve California, her eyaletteki kolluk kuvvetlerinin birbirlerine tanımlanamayan gizli avuç içi baskıları göndermelerine izin veren, eyalet çapında avuç içi baskı veri tabanları oluşturdu [48].

Şekil 4.21. Avuç İçi Tanıma Sistemi Örneği

El ve parmak geometrisini ölçen bu sistemlerde, el düz bir yüzeye yerleştirilerek hizalanır (Şekil 4.21). Ardından kamera, bir dijital TV uzaktan kumandasındaki gibi güvenli, kızılötesine yakın bir ışık kaynağı kullanarak elin birkaç fotoğrafını çeker ve sayısal bir şablona çevirir. Avuç içinde üç tür çizgi deseni açıkça görülebilir (Şekil 4.22). Bu çizgi desenleri Ana hatlar, Kırışıklıklar ve Sırtlar olarak bilinir. Ana hatlar; avuç içindeki en uzun, en güçlü ve en geniş çizgilerdir; avuç içindeki en ayırt edici özellikleri karakterize eder. Çoğu insanın Kalp Çizgisi, Kafa Çizgisi ve Yaşam Çizgisi olarak adlandırılan üç ana hat çizgisi vardır [50].



Şekil 4.22. Avuç İçi Baskıda Çizgi Desenleri [51]

Her insanda bu çizgilerden bulunuyor olsa da, elin açılması ve kapanması, yaş veya çevresel faktörler nedeniyle kişiler arasında büyük farklılıklar göstermektedir. Avuç kırışıklıkları, ana hatlardan daha ince ve daha düzensizdir. Sırtlar ise en ince ve en düzenli çizgilerdir ve parmak izlerinin kırışıklıklarına benzemektedir. Kırışıklık şekilleri bir kişiden diğerine farklılık gösterir, çünkü bunlar bir eğri veya paralel çizgiler olarak düşünülebilir [51].

Avuç içi tanımada, Görüntü işleme ve Özellik esaslı yorumlama olmak üzere iki temel yöntem bulunmaktadır:

- Görüntü işlemede; parmaklar görüntüden çıkarılarak avuç içi sınırları tespit edilir, gürültü yok etme, inceltme ve görüntüdeki kenar bilgilerinde oluşan kopuklukları ve çatallaşmaları gidermek amacıyla onarma işlemleri yapılır. Fourier dönüşümü veya Dalgacık dönüşümü gibi dönüştürme yöntemleriyle görüntü işlenir ve görüntüyü sayısal olarak niteleyen öznitelik verileri tespit edilir [52].
- Özellik esaslı yorumlama; avuç içi görüntü desenlerinde çizgilerle ayrılmış segmentlerdeki yapısal farklılıkların tespit edilmesi prensibine dayanır. Bu yaklaşımda Önişleme, Özellik çıkartma ve Eşleme olmak üzere üç aşama gerçekleştirilir [49]. Önişleme aşamasında; görüntü-

leme sisteminden alınan avuç içi görüntü resmi pekiştirilir, daha sonra segmentasyon ve binarizasyon işlemleri yapılır. Özellik çıkarma aşamasında; ön işlemleri tamamlanmış görüntüden karakteristik nokta ve yapılar tespit edilir. Bulunan bu özellikler Eşleme aşamasında kullanılır [49].

Damar kimlik doğrulama özellikli el tanıma teknolojisi ise, bir kişinin elindeki derinin altındaki damarların detaylarının okunmasını ve bu damarların önceden kaydedilmiş görüntülerle karşılaştırılmasını içerir. Biyometrik avuç içi damar tarayıcısı, kişinin avucunu kızılötesi ışınla tarayarak, damar yapısının özel bir kamera vasıtasıyla dijital bir fotoğrafını çeker, kişinin eşsiz damar modelinin dijital bir temsili olan benzersiz bir biyometrik şablon üretir. Damar kimlik doğrulaması güvenli kabul edilir, çünkü hiçbir insan aynı damar yapısına sahip değildir. Hatta sol ve sağ ellerde vasküler örüntüler de birbirinden farklıdır. Karmaşık damar yapısı insan vücudunda bulunduğundan, damar desenini kopyalamak veya çoğaltmak mümkün değildir. Ayrıca yağ ve kir, aşınma ve yıpranma, kuru ve ıslak el yüzeyi gibi dış koşullar damar yapısını etkilemez. İstikrar, teklik ve sahtekârlığa karşı dayanıklılık özellikleri, el damarını kişisel kimlik doğrulama için potansiyel olarak iyi bir biyometrik sistem hâline getirir [50].

Avustralya dünyadaki en büyük avuç içi baskı deposuna ev sahipliği yapmaktadır. Yeni Avustralya Ulusal Otomatik Parmak İzi Tanımlama Sistemi (NAFIS – National Automated Fingerprint Identification System) 4,8 milyondan fazla avuç içi izi içermektedir [48]. Yeni NAFIS, parmak izi veri alışverişi için ANSI/NIST uluslararası standardına uygundur, bu da Avustralya polis hizmetlerinin gerektiğinde Interpol veya FBI gibi denizaşırı polis kuvvetlerine parmak izi kayıtları sağlamasını kolaylaştırmaktadır.

Federal Soruşturma Bürosu (FBI - The Federal Bureau of Investigation) Ceza Adaleti Bilgi Hizmetleri (CJIS –Criminal Justice Information Services) Bölümü ise, dünyadaki en büyük ceza tarihi bilgileri koleksiyonuna sahiptir. Bu bilgiler, parmak izlerini Entegre Otomatik Parmak İzi Tanımlama Sistemi (IAFIS – Integrated Automated Fingerprint Identification System) aracılığıyla, federal yapıların, eyalet organlarının ve yerel kullanıcıların tanımlama hizmetlerine izin veren biyometrik sistem olarak kullanılır [48].

Avuç içi tanıma teknolojileri, kolay ve maliyeti düşük teknolojiler olduğundan uygulama açısından kolaylıklar içerir. Basit bir kullanıcı sistem etkileşimi sağladığı için sıfır veya çok küçük hatalı kayıt oranı elde edilebilir [53]. Ayrıca daha az sayıda veriyi daha kısa sürede işledikleri için işlem süresi kısadır. Bu sistemler parmak izi tanıma sistemlerinden daha güvenilir kabul edilir, çünkü kişinin damar yapısının okunması için hiçbir şeye dokunması gerekmez. Bunun yerine, tarama sırasında elin kısa süre okuyucunun üzerinde tutulması yeterlidir.

Çok sayıda insanın ellerini sayısız kez aynı sensöre yerleştirmek zorunda oldukları bu sistemde, birtakım hijyen sorunları oluşabilmekte, yüzeylerde kalan mikroplara dokunarak salgın hastalıkların yayılması hızlanabilmektedir. Aynı şekilde, bu sistemler kirden ve dış ortamlardan kolayca etkilenebilmektedir. Sensörün yüzeyinde kalan gizli el izlerinin kopyalanabilme ihtimali ise bir diğer sorundur. Araştırmacılar, sahte parmakların kalıplarını ve gizli parmak izlerini kullanmak için sistematik yöntemler geliştirmişlerdir [54].

4.3. BİYOMETRİK VERİLERİN KARŞILAŞTIRILMASI

Yukarıda incelenen Biyolojik Biyometrik Sistemler birbirlerinden farklı özelliklere sahip olup, her birinin performansı ve verimliliği kullanım alanlarına göre değişiklik göstermektedir. Bu konuyla ilgili aşağıda farklı sınıflandırmalar ve karşılaştırmalar gösterilmiştir (Tablo 4.1, 4.2, 4.3 ve 4.4).

Tablo 4.1. Biyometrik Teknolojilerin Kullanım Kolaylığı, Kullanım Sorunları, Doğruluk ve Güvenlik Gereksinimi Açısından Karşılaştırılması [55]

BİYOMETRİK SİSTEM	KULLANIM KOLAYLIĞI	SORUNLAR	DOĞRULUK	GÜVENLİK GEREKSİNİMİ
PARMAK İZİ	Yüksek	Kuruluk, kir ve yaş	Yüksek	Yüksek
YÜZ	Orta	Işık, yaş, gözlük, saç	Yüksek	Orta
İRİS	Orta	Işık	Çok Yüksek	Çok Yüksek
RETİNA	Düşük	Gözlük	Çok Yüksek	Yüksek
EL GEOMETRİSİ	Yüksek	Elde hasar, yaş	Yüksek	Orta

Tablo 4.2. Biyometrik Teknolojilerin Ayırt Edicilik, Evrensellik, Kalıcılık, Ölçülebilirlik, Performans, Kabul Edilebilirlik ve Aldatılabilirlik Açısından Karşılaştırılması [56]

	Ayırt Edicilik	Evrensellik	Kalıcılık	Ölçülebilirlik	Performans	Kabul Edilebilirlik	Aldatılabilirlik
PARMAK İZİ	Yüksek	Orta	Yüksek	Orta	Yüksek	Orta	Orta
YÜZ	Düşük	Yüksek	Orta	Yüksek	Düşük	Yüksek	Yüksek
İRİS	Yüksek	Yüksek	Yüksek	Orta	Yüksek	Düşük	Düşük
RETİNA	Yüksek	Yüksek	Orta	Düşük	Yüksek	Düşük	Düşük
DNA	Yüksek	Yüksek	Yüksek	Düşük	Yüksek	Düşük	Düşük
AVUÇ İÇİ	Orta	Orta	Yüksek	Orta	Yüksek	Orta	Orta

Tablo 4.3. Biyometrik Teknolojilerin Uygulama Alanları [57]

	Parmak İzi	Yüz	İris	Retina	El Damar Örüntüleri	Parmak Eklem İzi	El Geometrisi	Avuç İçi
Sınır Kontrol	+	+	+	+				
Adli Bilişim	+	+						
Suçlu Tanıma	+	+	+	+				
Kimlik Kartı	+	+	+					
Pasaport	+	+	+					
Bilgisayar Oturum Açma	+	+	+		+	+	+	+
Erişim Kontrolü	+	+	+	+	+	+	+	+
E-Ticaret	+	+	+		+	+	+	+
Akıllı Telefon	+				+		+	+
Görüntüleme Sistemleri	+		+			+	+	+
Video İzleme		+						
Kayıp Çocuk Tanıma	+	+	+					
Kalabalık Görüntüleme		+						
E-Banka								

Tablo 4.4. Biyometrik Tanıma Sistemlerinin Çeşitlerinin Taradıkları Özelliklere Göre Sınıflandırılması [53]

Biyometrik Karakteristik	Sistemin Taradığı Özelliklerin Açıklaması
Parmak İzi	Parmak satırları, gözenek yapısı
Yüz geometrisi	Göz, burun vs. arası uzaklıklar
İris Tanıma	İris deseni
Retina	Retina yapısına (desenine) göre
El Geometrisi	Parmak ve avuç içi ölçülerine göre
El Damar yapısı	Elin arkası, parmak veya avuç içi damar yapısı
DNA	Kalıtsal bir taşıyıcı olan DNA

Biyometrik sistemleri kullanacak kişi veya kuruluşlar, öncelikle bir sistemde en çok hangi özellikten faydalanmak istediklerine karar vermelidir. Örneğin, Tablo 4.1'e göre, eğer güvenliği ön planda tutacaklarsa iris taramanın en güvenilir olduğu; doğruluğu tercih ediyorlarsa iris ve retina taramanın en yüksek doğruluk oranına sahip olduğu görülecektir. Tablo 4.2'ye göre kabul edilebilirlik ve aldatılabilirlik ihtimalinin en düşük olduğu sistem yüz tanıma olarak belirtilmişken, performans ve ayırt edicilik bakımından en düşük özellikte olan sistemin yine yüz tanıma olduğu görülmektedir. Tablo 4.3'te uygulama alanları bakımından en tercih edilen sistemlerin parmak izi ve yüz tanıma olduğu, iris tanımanın ise onları takip ettiği anlaşılmaktadır. İhtiyaca ve amaca uygun olarak hangi sistemin seçileceğine karar verildikten sonra, farklı biyometrik sistemlerin insan fizyolojisinde hangi özellikleri taradığı ise Tablo 4.4'te gösterilmiştir.

Yapılan iş ve saklanan veriye göre değişkenlik gösterecek olan teknoloji ihtiyacı bu sistemlere olan talebi ve beklentiyi farklılaştıracaktır ancak kuşkusuz ki hepsi için ortak olan temel ihtiyaç, saldırganların hedefi olmaktan kurtaracak ve var olan verileri koruyacak yüksek güvenlik olacaktır. Kişilerin ve kurumların veri güvenliğini sağlamak, kamu güvenliğinin de temel taşı olduğundan, bu sistemlerin başarısı büyük önem arz etmektedir.

4.4. BİYOMETRİ VE KAMU GÜVENLİĞİ

Devletler yıllardır vatandaşlarının gözlerinin veya saçlarının rengi, yüz özellikleri, boyu, kilosu ve diğer temel fiziksel özelliklerin fiziki kayıtlarını biyometrik veri olarak toplamaktadır. Polis yüzyılı aşkın süredir olay mahallinde bırakılan parmak izlerini analiz etmekte ve zamanla şüphelilerle/suçlularla ilişkili parmak izi kayıtlarını genişletmektedir. Parmak izleri önceleri fiziksel olarak karşılaştırılırken, bugün bilgisayarlar bu işlemi devralmıştır. Otomatik Parmak İzi Tanımlama Sistemi (AFIS), bir suç mahallinde bulunan izleri, milyonlarca depolanmış parmak izi görüntüsüyle sadece birkaç saniyede karşılaştırmaktadır.

Biyometrik teknolojiler, şüpheli kişileri tespit ederek yürütülen soruşturmaları kolaylaştırır veya suçlu olmayan ve kimliğinin tanımlanması gereken kişilere erişim izni verebilir. Amaç, kamu alanlarının ve kritik altyapıların güvenliğinin sağlanmasıdır.

Kamu güvenliği için genel kullanım alanları olarak;

- Sınır kapılarında veya havaalanlarında yolcuların giriş çıkışları sırasında hızlı ve otomatik işlem yapılması ile kişilerin kimliğini tanımlamada güvenilir kontrol için,
- Kolluk kuvvetleri açısından kimlik kontrolleri, videolardan kişi analizleri için,
- Halkın kullandığı ortak alanlara veya kritik altyapılara güvenli erişim sağlanması için, parmak izi veya yüz tanıma erişim sistemlerinin kullanılması.

Sınır kontrolü konusunda, sınırlardan gelip geçen insan sayısının çokluğu sebebiyle, kontroller de sıklaşmakta, bunun için işlemlerin hızlı ve güvenilir şekilde yürütülmesi gerekmektedir. Bu konuda ülkeler biyometrik pasaport uygulamasına geçmeye başlamışlardır. Biyometrik pasaportların benimsenmesini ve uluslararası alanda birlikte çalışabilirliğini teşvik etmek için, Uluslararası Sivil Havacılık Örgütü (ICAO- The International Civil Aviation Organization*)* üç standart biyometrik özelliğin kullanılmasını tavsiye etmiştir: parmak izi taraması, yüz tanıma ve iris taraması. Bunlar şu anda en yaygın kullanılan biyometrik teknolojileri temsil etmektedir [1].

ICAO'ya göre üç zorunlu biyometrik pasaport (e-Passport) türü vardır [58]:

- Temel Erişim Kontrolü (BAC - Biometric Access Control) ile Biyometrik Pasaportlar: Biyografik verilerin, iris ve yüz görüntülerinin güvenli bir şekilde okunmasını sağlar.
- Genişletilmiş Erişim Kontrolü (EAC - Extended Access Control) ile Biyometrik Pasaportlar: Hem isteğe bağlı hem de zorunlu biyometrik özellikler de dâhil olmak üzere, oldukça hassas biyometrik verilere erişimi kısıtlayan ikinci nesil bir mekanizmadır. Bu pasaport asimetrik şifreleme protokollerine dayanır ve daha güçlü şifreleme kullanır.
- Ek Erişim Kontrolü (SAC - Supplemental Access Control) ile Biyometrik Pasaportlar: İsteğe bağlı ve zorunlu biyometrik özellikler de dâhil olmak üzere, son derece hassas biyometrik verilere erişimi daha da kısıtlayan üçüncü nesil Şifre Doğrulama Bağlantı Kuruluşu (PACE Password Authenticated Connection Establishment)'dur. Asimetrik şifreleme uygular ve veri şifrelemesini okuma cihazı ile çip arasında paylaşılan bir anahtara dayandırır.

Sınır Ötesi Biyometrik Bilgi Akışı (TBIF – Transborder Biometric Information Flow) verilerine göre, uluslararası biyometrik anlaşmalara ve endüstriye yönelik standartlar, çoğunlukla iki örgütün; Uluslararası Sivil Havacılık Örgütü (ICAO) ve Uluslararası Göç Örgütü (IOM - the International Organization of Migration)'nün çabalarına dayanmaktadır. Diğer iki bölgesel örgüt; Avrupa Birliği (AB) ve Asya Pasifik Ekonomik İş Birliği (APEC – the Asia Pacific Economic Cooperation) biyometrik sınır kontrol sistemleri için sınırlı bir rol oynamıştır [58].

Göç kontrolü için biyometrik sistemlerin kullanılması, kişilerin kimliklerini toplamak ve kaydetmek için yenilikçi yöntemlere, gelişmiş güvenlik ve sınır kontrol noktalarında verimliliği arttırmaya genellikle yardımcı olmuştur [58]. Bu tedbirler aynı zamanda yasadışı göçü durdurmayı, sınır ötesi suçlarla mücadeleye yardımcı olmayı ve terörizmi önlemeyi amaçlamaktadır. Bununla birlikte, göç kontrolü için biyometrik sistemlerin, yasadışı göçü, sınır ötesi suçları ve terörizmi durduramadığı görülmektedir [58].

Teknoloji geliştikçe kimlik tanıma da elektronik hâle gelerek, daha hızlı ve daha kolay hareket etmekte ve insan tabanlı analizden daha kesin çözümler sunmaktadır. Öyle ki, CCTV (Kapalı Devre Televizyon – Close Circuit Tele

Vision) ve MOBESE (Mobil Elektronik Sistem Entegrasyonu) kayıtlarından, veri tabanı kayıtlarından veya sosyal medyadaki fotoğraflardan kişiler kolaylıkla tespit edilebilmektedir. Dahası sosyal platformlar, kolluk kuvvetlerinin şüphelilerin fotoğraflarını bulmasına ve lokasyonlarını tespit etmesine izin vermektedir. Bununla birlikte, sosyal medya verileri tarafından yönlendirilen yüz tanıma, terörle mücadele ve hatta kayıp çocukları bulmak için kullanılmaktadır.

Kamu güvenliği, ulusal güvenlik ve suçla mücadele amacıyla kullanılan biyometrik teknolojiler, gizlilik ve veri koruma hakları dâhil, yasal, politik ve etik konular göz önüne alınarak üretilmeli ve işletilmelidir. Ülkelerin ulusal güvenlikteki kamu çıkarlarını, bireylerin sivil hakları ve özgürlükleri ile doğru bir şekilde dengelemeleri gerekmektedir. Bu da bizi sivil kimlik ve özel veri güvenliği konularına getirmektedir.

4.5. BİYOMETRİ VE SİVİL KİMLİK

Sivil kimlik, devlet kurumlarıyla etkileşimde bulunurken kişilerin kimliğini tanımlamak veya doğrulamak için kullanılır. Bir devletin ana görevlerinden biri, vatandaşlarının kimliğini güvence altına almaktır. Dünyanın her ülkesinde vatandaşlar, kim olduklarını kanıtlamak, banka hesabı açmak, sağlık hizmetlerinden yararlanmak, okula veya kurslara kaydolmak, oy kullanmak veya sosyal yardımdan yararlanmak gibi sosyal hayatı ve iş hayatını düzenleyen birçok işlemi yapmak için devlet tarafından verilen kimlik belgelerine bağımlıdır. Kimlik, bizim kim olduğumuzun göstergesidir.

Vatandaşların kimlik kayıtlarının doğru bir şekilde tutulması, güçlü ve çok faktörlü kimlik doğrulamaları kullanılması, özellikle büyük nüfuslu ülkeler düşünüldüğünde, üzerinde dikkatle durulması gereken bir konudur. Toplumun ve ekonomilerin teknoloji tabanlı dijital dönüşümü, ülkeleri, vatandaşlarını kimlik hırsızlığına karşı korumak ve güvenli, çevrimiçi hizmetler sağlamak için çalışmaya ve önlemler almaya zorlamaktadır. Bu ihtiyacı da günümüzde biyometrik teknolojiler karşılamaya yardımcı olmaktadır. Fiziksel ve dijital olarak kimlik hırsızlığı riskini azaltarak, güvenli ve pratik kullanımı sağlamak için yeni kimlik yönetimi hizmetlerinin uygulanmasını kolaylaştırmayı hedeflemektedir. E-kimlik kartları, biyometrik pasaportlar

ve e-ehliyetler gibi güvenli kimlik belgeleri uygulamalarına geçilmesi bunlardan bazılarıdır.

Vatandaşların kimliklerine yönelik bireysel saldırılar kadar, hükümetlerin çevrimiçi sistemlerine yönelik daha geniş çaplı saldırılar, hem kişi güvenliğini ciddi tehlikelere maruz bırakırken, hem de devletlerin iç işleyişlerinde karışıklığa neden olabilmektedir. Saldırganların sisteme erişim elde etmesi veya biyometrik verileri taklit etmesi, devletin sağlık ve finans endüstrileri gibi çok fazla alanını risk altına sokmaktadır. Bu sebeple ulusal kimliklerin güncel ve doğru bir kaydını tutmak ve bunları korumak çok önemlidir.

Kimlik tespitleri, bireyler ve hükümetler veya özel kurumlar arasında yapılandırılmış bir toplumda faaliyet göstermenin kolaylaştırılmasında önemli bir rol oynamaktadır. Kişinin kimliğini kanıtlayamaması neticesinde, temel haklarını kullanması ve bu haklarını talep etmesi, çeşitli devlet hizmetlerine erişmesi ve birçok günlük faaliyeti yürütmesi de mümkün olamayacaktır. Her ülkenin kendi nüfus popülasyonlarının büyüklüğü düşünüldüğünde, belli bir kişiyi tanımlamak ve iddia ettiği kişi olup olmadığına ilişkin kimlik doğrulaması yapmak oldukça önemlidir. Ancak kimlik yönetimi artık sadece kimlik kartı vermekle ilgili değildir, biyometrik sistemler vasıtasıyla toplanan çok miktardaki kişisel ve hassas verinin korunması ve yönetimi de göz ardı edilmemelidir.

4.6. BİYOMETRİ VE ÖZEL VERİ GÜVENLİĞİ

Biyometrik veri, bilgi sistemlerinde saklanabilen ve biyometrik sistemler tarafından işlenebilen dijital bir veridir. Bu biyometrik veriler, herhangi bir saldırı sonucunda ele geçirilmesinin engellenmesi amacıyla şifreli bir biçimde saklanır. Rakam veya harften oluşan klasik şifreler ele geçirildiğinde, şifreyi değiştirmek zararın oluşmasını önleyebilir veya azaltabilirken, biyometrik sistemlere yapılan saldırılarda biyometrik veriler değiştirilemediği için çok ciddi zararlara neden olabilmektedir. Bu sebeple biyometrik sistemlerin ve bu sistemler yoluyla elde edilen biyometrik verilerin güvenliği çok önemlidir.

Biyometrik tanımlama ve doğrulama, mutlaka bir biyometrik veri tabanındaki bir veri kaydı ile gerçekleştirilmez. Biyometrik veriler **e-**kimlik kartı veya

pasaport, akıllı telefon vb. içine yerleştirilmiş bir çipte de saklanabilir. Böyle bir durumda, kimlik doğrulama işlemi söz konusu olduğunda, çipteki veriler kartın veya pasaport taşıyıcısının fiziksel verileri ile karşılaştırılır.

Verilerin ele geçirilmesi, her zaman elektronik sistemlere yapılan saldırılar yoluyla olmamakta, örneğin fotoğraf, video, belge gibi kişisel bilgilerden oluşan eski sabit diskin imha edilmeden çöpe atılması, kurumsal ortamlardaki zayıf parolalar, bilgisayar ve ağ güvenliğine yönelik yetersiz uygulamalar da veri ihlallerine yol açabilmektedir. Sosyal mühendislik yöntemleri uygulamak, bilgisayar korsanlığı yapmak, donanım cihazlarını çalmak gibi çok sayıda yöntemle veya kişilerin ya da kurumların cihazları kaybetmesi veya bilgileri yeterince koruyamaması neticesinde de çok sayıda önemli bilgi ele geçirilmektedir.

Biyometrik verileri depolamak için, uygulama türüne ve gereksinimlerine bağlı olarak, yaygın olarak kullanılan biyometrik veri depolama yöntemleri [59]:

- Taşınabilir Aygıt (akıllı kart vs. maliyetlidir, çünkü biyometrik akıllı kart okuyucusu gereklidir),
- Merkezî Biyometrik Veri Tabanı (ucuzdur fakat biyometrik veriler genellikle ağ üzerinden aktarıldığından güvenlik riski vardır. Şifreleme sorunları da bulunmaktadır),
- Bireysel İş İstasyonları (veriler çeşitli iş istasyonları arasında dağıtılarak güvenliği sağlanmaya çalışılır ancak merkezî veri tabanına göre çoğu zaman daha az güvenli olma ihtimali taşıyabilmektedir).

Yurt içinde biyometrik veri tabanlarının oluşturulması, gizlilikle ilgili yasal zorlukları ve etik endişeleri arttırmaktadır; örneğin, verilere kimlerin erişebildiği; merkezî veri tabanlarında yer alan veri bütünlüğü; üçüncü şahıslar için veri koruması; ayrımcılık sorunları; veri depolama kısıtlamaları; verilerin suç kontrolü amacıyla kullanılması ve mahremiyet üzerindeki etkisi vb. Uluslararası düzeyde, mahremiyetle ilgili yasal zorluklar daha da artmaktadır [58], çünkü mahremiyet ve veri koruma üzerindeki etkisi, ulusal veri tabanlarında listelenenlere kıyasla daha geniş bir yelpazeyi etkilemektedir ve tüm ülkeler farklı antlaşma ve anlaşmalarda yer alan mahremiyet haklarına tam olarak bağlı değildir [58].

Biyometrik sistemlerden toplanan verilerin ne kadar süreyle saklanacağı, güvence altına almak için hangi aşamaların uygulanacağı, üçüncü kişilerle

paylaşılıp paylaşılamayacağı ve yasa uygulayıcılarının bir biyometrik veri tabanını taramak için hangi standartları uygulaması gerektiği konularında detaylı düzenlemeler gereklidir. Çünkü biyometrik veri özel ve riskli bir bilgidir, çalınması veya tehlikeye girmesi durumunda iptal etmek veya yeniden düzenlemek mümkün değildir. Eğer kolluk kuvvetleri, topladıkları biyometrik verileri, üçüncü kişilerce yönetilen veri tabanlarında saklıyorsa, bu üçüncü kişilere, bu verilerine erişebilme ve bu verileri kontrol edebilme imkânını da sundukları göz ardı edilmemelidir.

4.7. BİYOMETRİK KORSANLIK

Her kimlik doğrulama yöntemi için risk bulunmaktadır. Biyometrik teknolojiler, zayıf ve kolayca kırılabilen, unutulup kaybedilebilen, başkalarıyla paylaşılabilen ve tekrar kullanılan şifreler için daha güvenli bir alternatif gibi görünebilir ancak bir sızıntı sonucunda ele geçirildiğinde değiştirilmesi mümkün değildir. Bir saldırganın biyometrik verilere erişmesi ve bu verileri kendi yararına kullanması karşılaşılan bir durumdur.

İster yüz tanıma sistemlerinden gelen yüz fotoğrafları, ister tarayıcılardan gelen parmak izleri olsun tüm biyometrik veriler, bir noktada, bir bilgisayar sisteminde, bir veri tabanında veya taşınabilir bir depolama aygıtında saklanabilen bir dijital formata dönüştürülür. Sırf bu sistemlerin savunmasız bırakılması sebebiyle bile biyometrik verilerin ele geçirilmesi söz konusu olabilmektedir. Diğer taraftan, kullanılan her güvenlik sisteminde olduğu gibi, biyometrik tabanlı güvenlik sistemlerinde de sistemin kullandığı herhangi bir yazılıma ya da donanıma yapılabilecek saldırılar mevcuttur [16].

Biyometrik teknolojilere sistemin özelliğine göre farklı türde saldırılar yapılabilmektedir. Örneğin, eğer saldırganın cihaza fiziksel erişimi mümkünse, gerekli ayarları yaparak sistemin kendi kimliğini doğrulamasını sağlayabilir veya ele geçirilen verileri başka sistemlerde tekrar kullanarak o sistemlerde kimlik doğrulaması yapabilir.

Sahte ya da kopyalanmış biyometrik bilgileri kullanarak, bir biyometrik güvenlik sistemini kandırma riski de gelişen teknolojiyle artmaktadır. Örneğin, akıllı telefonları veya tabletleri açmak için kullanılan yüz tanıma sistemleri, sahibinin fotoğrafı gösterilerek aldatılabilir. Veya saldırganlar, bir parmak

izini yapay bir silikon üzerine kopyalayarak veya kalıplandırarak, bir mobil cihazın kilidini açabilir veya pek çok sisteme erişim sağlayabilirler.

Şirketler, bilgisayar korsanlarının bir adım önüne geçmek için sürekli yeni çalışmalar yapmaktalar ancak kişiler rutin yeme içme faaliyetleri neticesinde çok sayıda nesneye tükürük, parmak izi ve DNA'larını bırakmakta ve hırsızlık için sayısız fırsat sunmaktalar.

Kişisel, kamusal veya ülkesel alanda güvenliğin teknolojiyle birlikte artan önemi neticesinde, aynı hatta belki daha büyük hızla artan korsanlık faaliyetleri sebebiyle, uzmanlar da güvenlik açıklarını tespit etmeye yönelmişlerdir. Bu hususta örnek vermek gerekirse;

- Ergonomik nedenlerden dolayı, çoğu parmak izi okuyucusunun, parmağın tamamı yerine bir kısmını taraması sebebiyle, karşılaştırma sırasında kısmi kayıtlar kullanılmaktadır. Ayrıca, parmak izleri bazı yaygın özellikler de taşımaktadır. Bu sebeplerle, New York Üniversitesinden Philip Bontrager ve araştırma ekibi, mümkün olduğunca çok sayıda kısmi parmak iziyle eşleşen yeni parmak izleri oluşturmak için bir makine öğrenme tekniği kullandılar ve "DeepMasterPrint" olarak adlandırdılar. Sinir ağlarını öğrenmek ve optimize etmek için girdi olarak NIST'in veri tabanından yararlandılar. Bunun sonucunda, üretilen parmak izinin akıllı telefon, tablet ve hatta ev güvenlik sistemi gibi yalnızca tek bir kimlik doğrulama rutinine sahip cihazlara giriş yapabileceğini keşfettiler [60].
- 2018 yılında, Almanya'nın Leipzig kentinde düzenlenen "Chaos Communication" konferansında, güvenlik araştırmacıları Jan Krissler ve Julian Albrecht, hem Hitachi hem de Fujitsu tarafından üretilen tarayıcıları sahte el kullanarak nasıl atlatabildiklerini gösterdiler. Bunun için kızılötesi filtresi devre dışı bırakılmış bir kamerayla kendi ellerinin fotoğraflarını çektiler. Kesin sonuç elde etmek için 30 gün boyunca 2.500'den fazla fotoğraf denemesi yapıldığı belirtildi. Daha sonra bu görüntüyü, bir kâğıda normal bir el boyutunda olacak şekilde bastırdılar, yazdırılan görüntüyü balmumu ile kapladılar ve bunu bir eli simüle etmek için kullandılar.

Bahsi geçen şekillerdeki aldatmalardan korunmak ve biyometrik teknolojilerin, ölü kişilerin veya başka şekilde etkisiz kılabilecek yöntemlerle kullanıcı-

ların fotoğraflarını ya da videolarını doğrulamamasını sağlamak için "canlılık tespiti" gereklidir [61]. Bu nedenle, biyometrik canlılık tespiti genellikle parmak izi taramalarında vücut sıcaklığının kontrol edilmesini veya ses tanımada potansiyel çalma yankısını içerir; yüz tanımada bulanıklık veya bozulma ve özellik eşleşmesi arar. Bu sayede yapay, protez, sahte ya da cansız organlar kullanma imkânı ortadan kalkmış olur. Saldırganların sahte ses veya video üretmeye odaklanırken, canlılık algoritmasını atlatmaları gereklidir [61].

Canlılık algılama yöntemleri, kullanıcılardan gözlerini kırpmasını, gülümsemesini, başını sallamasını, renkli yanıp sönen ışıkları izlemesini, rastgele yüzler yapmasını, rastgele konuşmasını ve çok daha fazlasını istemektedir ancak bu eski tekniklerin çoğunun "Deepfakes" tarafından kolayca taklit edildiği görülmektedir. Deepfakes en genel tanımıyla, mevcut bir görüntüde veya videoda yer alan bir kişinin, yüz ifadelerinin, tavırlarının veya sesinin, yapay sinir ağları, yüz haritalama teknolojisi ve yapay zekâ kullanılarak, bir başka kişinin görüntüsü ile değiştirildiği, taklit edilebildiği bir medya türüdür ve derin öğrenme (deep learning) ve sahte (fake) kelimelerden türetilmiş bir birleşik kelimedir [62]. Şimdilerde çok sayıda sosyal medya platformunda eğlence amaçlı kullanıldığına şahit olduğumuz bu uygulamaların, yakın gelecekte daha kaliteli görüntüler üreteceği, insan sesini taklit edecek kadar gelişeceği ve canlılık tespiti olanlar da dâhil olmak üzere, birçok yüz tanıma sistemini geçecek kadar başarılı olacağı uzmanlarca belirtilmektedir. Yazılımın, özellikle biyometrik özçekim verilerinin önümüzdeki yıllarda karanlık ağda daha kolay erişilebilir olması sonucunda, kimlik hırsızlığını gerçekleştirmek için giderek daha fazla kullanılacağı da vurgulanmaktadır. Bu açıdan, zararlı kullanımın önlenmesi için daha güçlü güvenlik tedbirlerine, üretim, dağıtım ve kullanım durumları için daha detaylı hukuki düzenlemelere ihtiyaç duyulacağı açıktır.

Geçtiğimiz yıl**,** biyometrik güvenlik firması Biostar 2 tarafından, bir milyondan fazla parmak izi ve diğer hassas verilerin açığa çıktığı belirtildi. Araştırmacılar açığa çıkan veriler arasında ayrıca, kişilerin fotoğraflarının, yüz tanıma verilerinin, isimlerinin, adreslerinin, şifrelerinin, istihdam geçmişlerinin ve güvenli alanlara ne zaman eriştiklerini gösteren kayıtların bulduğunu söylediler. Birleşik Krallık Büyükşehir Polisi de dâhil olmak üzere dünya çapında binlerce şirket tarafından güvenli tesislerin belirli bölümlerine erişimi kontrol etmek için kullanıldığı düşünüldüğünde, milyonlarca verinin kontrolsüzce or-

talıkta dolaştığı ve bunun sonucunda işletmelerin, kuruluşların ve çalışanların büyük bir risk altında olduğu açıktır.

Bilgisayar korsanları, sadece biyometrik kimlik doğrulama donanımı ve cihazlarında bulunan kusurlardan değil, aynı zamanda verilerin toplanması ve depolanmasından da yararlanmayı hedeflemektedir. Yavaş yavaş hayatımıza girmeye başlayan biyometrik sistemler, ihtiyaçlar doğrultusunda daha da yaygınlaşacak ve bunun sonucunda da siber suçlular için daha fazla değer kazanacak ve hırsızlık, sahtekârlık riski de daha fazla artacaktır. Bu sebeple, bu risklerden korunmak için, biyometrik veriler güçlü şifrelerle şifrelenmeli ve güvenli sunucularda saklanmalı, sensörler, tarayıcılar ve diğer donanımların anormallikleri daha iyi tespit edinceye kadar, biyometri çok faktörlü bir kimlik doğrulama sisteminin bir parçası olarak kullanılmalıdır. Bu kapsamda, saldırganlardan bir adım önde olmak isteyen her devletin ve her kuruluşun bilinçlendirilmesi ve eğitilmesi ana amaç hâline getirilmelidir.

4.8. HUKUKİ DÜZENLEMELER

Biyometrik teknolojinin yaygınlaşması, çok sayıda biyometrik verinin kontrolsüz bir şeklide toplanmasına ve işlenmesine neden olurken, insan hakları, özel hayatın gizliliği, temel hak ve özgürlükler, ayrımcılık yapmama ve savunmasız grupların korunması gibi pek çok konuda da bazı soruları gündeme getirmektedir. Bu kapsamda, biyometrik verilerin gizliliğinin sağlanmasını, temel hak ve özgürlüklere saygı duyulacak şekilde yönetimini, kuruluşların biyometrik verilerin toplanması, saklanması, kullanılması ve paylaşılması ile ilgili konularda uyacakları standartları ve yasal düzenlemeleri hazırlamak da artık kaçınılmaz olmuştur.

Bireylerin bilgisi veya onayı olmadan bir kalabalığın içindeki tüm yüzlerin taranarak biyometrik verilerin toplu olarak toplanması ve saklanması, gizlilik hakkında birçok endişeyi de beraberinde getirir. Güçlü yasal çerçevelerin ve katı önlemlerin yokluğunda, biyometrik teknolojiler, ayrımcılık, profil oluşturma ve kitlesel gözetimi kolaylaştırmak için uygulamaları genişletebildiğinden, gizlilik ve kişisel güvenliğe karşı ciddi bir tehdit oluşturmaktadır.

Artan dijital hayat, işlerin de dijital ortamdan yürütülmesine sınırsız imkân sağlamakta, iş dünyasında ve ticari platformda, iş sahiplerinin; çalışanlarının, müşterilerinin veya iş ortaklarının her zamankinden daha fazla biyometrik verisinin toplamasına ve bu verileri ticari amaçlar için kullanmasına yol açmaktadır. Buna rağmen, çoğu iş sahibi, işine yarayıp yaramadığına bakmadan topladıkları bu verileri maliyetten tasarruf etmek için yetersiz veri güvenliği önlemleriyle depolamayı veya işlemeyi tercih etmektedir.

Bu bağlamda, kişisel verilerin gizli tutulmasının ve kötüye kullanılmamasının, yalnızca gerektiğinde ve yasal olduğu ölçüde toplanmasının son derece önemli olduğu devletlerce fark edilmeye başlanmıştır. Yapılan düzenlemelerde, toplanan kişisel verilerin; bir kanuni gerekçeye dayandırılma, kişisel verisi işlenen ilgili kişinin bilgisi ve açık rızası ile toplanma, doğru, eksiksiz ve güncel olmasını sağlama konularında uyarılar içerdiği görülmektedir. Bununla da yetinilmeyerek, saklanan verilerin güvenliğini sağlamak ve yetkisiz erişimi önlemek için etkili idari ve teknik tedbirlerin alınması gerektiği de açıkça belirtilmektedir.

Kişisel verilerin korunmasına yönelik ilk hukuk düzenlemeleri; 1970 yılında Almanya, 1973 yılında İsveç ve 1974 yılında ABD'de yapılan yasa metinleri olarak ifade edilmektedir [63]. Avrupa'da 1980'li yıllardan itibaren, başta İktisadi İş Birliği ve Kalkınma Teşkilatı'nın (OECD –Organisation for Economic Cooperation and Development) "Özel Hayatın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri" ile Avrupa Konseyi'nin "*108 no'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi*"; 90'lı yıllarda Birleşmiş Milletlerin "*Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri*" ile "*95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Direktifi*"; 2000'li yıllarda "*181 no'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınır Aşan Veri Akışına İlişkin Protokol*" ve nihayet *2016/679 Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR*) ile kişisel verilerin korunması hakkı hukuki alanda kabul edilmiştir.

Amerika Birleşik Devletleri'nde ise, biyometrik bilgi gizliliğinin yasal çerçevesi olan Illinois Biyometrik Bilgi Gizliliği Yasası (BIPA - Biometric Infor-

mation Privacy Act) 2018 yılında kabul edilmiştir. BIPA'ya ek olarak, diğer eyaletlerden Texas 2009'da, Washington 2017'de biyometrik bilgi gizliliği yasalarını onayladı [64]. BIPA, diğer kişisel veriyle ilgili düzenlemelerde olduğu gibi, biyometrik tanımlayıcıların ve bilgilerin toplanmasını, kullanılmasını, korunmasını, işlenmesini, depolanmasını, saklanmasını ve imha edilmesini düzenlemeye yardımcı olmak için hazırlanmıştır.

California Tüketici Gizlilik Yasası (CCPA - California Consumer Privacy Act), GDPR'a benzer şekilde "biyometrik verileri" tanımlamakta olup, tüketicilerin izni olmadan işletmeler tarafından toplanan biyometrik verilerin kamuya açık bilgiler olmadığını açıkça belirtmektedir. CCPA, DNA, iris ve retina taramaları, parmak izleri, damar örüntüleri, ses kayıtları ve tanımlayıcı bilgiler içeren uyku, sağlık veya egzersiz verilerini düzenlemekle birlikte, GDPR'dan farklı olarak, biyometrik veriler için ayrı veya daha fazla koruyucu bir düzenleme içermemektedir.

4.8.1. GDPR (General Data Protection Regulation – AB Genel Veri Koruma Tüzüğü)

Kişisel verilerin korunması alanında AB'de 1995 yılında yürürlüğe giren 95/46/EC sayılı AB Veri Koruma Direktifi, daha sonradan ihtiyaçlar doğrultusunda genişletilip güncellenmiş ve Avrupa Parlamentosu tarafından 14 Nisan 2016 tarihinde "Genel Veri Koruma Tüzüğü (GDPR - General Data Protection Regulation)" adını almıştır ve 25 Mayıs 2018'den itibaren yürürlüktedir. GDPR'ın yürürlüğe girmesinin ardından, 95/46/EC sayılı AB Veri Koruma Direktifi yürürlükten kalkmış olup, bu tarihten itibaren söz konusu GDPR hükümleri, küresel anlamda nerede hizmet verdiğine ve faaliyette bulunduğuna bakılmaksızın, GDPR'ın uygulama alanındaki her veri sorumlusu/veri işleyen bakımından bağlayıcı olup, işleme konu her kişisel verinin de hukuki güvencesini sağlamayı amaçlamaktadır.

GDPR kapsamında biyometrik veriler "Hassas Veri" kapsamında sayılmakta ve daha yüksek koruma ve gizlilik öngörülmektedir.

Tüzüğün kapsamına bakıldığında md. 4/14'te Biyometrik Veri kavramı:

> *"yüz görüntüleri veya daktiloskopik veriler gibi bir gerçek kişinin özgün bir şekilde teşhis edilmesini sağlayan veya teyit eden fiziksel,*

fizyolojik veya davranışsal özelliklerine ilişkin olarak spesifik teknik işlemeden kaynaklanan kişisel veriler" olarak tanımlamaktadır.

Md 9/1 uyarınca ise; "…*bir gerçek kişinin kimlik teşhisinin yapılması amacıyla genetik veriler ile biyometrik verilerin işlenmesi yasakt*ır." denmektedir. Bir verinin biyometrik veri kapsamında değerlendirilebilmesi için o verinin sadece o kişiyi tanımlayabilme ya da doğrulayabilme özelliğine sahip olması gerekir.

Bir biyometrik verinin işlenebilmesi için, verinin işlendiği ülkenin ulusal mevzuatlarında veya Avrupa Birliği mevzuatı uyarınca hukuka ve işleme amacına uygun bir faaliyette bulunması gerekmektedir. Eğer bu hususta herhangi bir madde kapsamına girmiyorsa, biyometrik verisi işlenen kişinin açık rızasının alınması gerektiği tüzükte düzenlenmiştir. Hiçbir kişisel veri, tüzükte belirtildiği şekilde yapılmadığı veya ilgili kişiden (kişisel veri sahibinden) açık bir onay almadığı sürece işlenemez. İlgili kişi bu izni istediği zaman iptal etme hakkına sahiptir.

95/46 sayılı Direktifinin temel dayanağı esasen, Avrupa İnsan Hakları Sözleşmesinin 8. maddesiyle koruma altına alınan "Özel Hayatın Gizliliği ve Ailenin Korunması Hakkı" ile AB Temel Haklar Şartı'nda yer alan "Özel Hayat ve Aile Hayatına Saygı Hakkı (madde 7)" olup, GDPR de bu temel üzerinden oluşturulmuştur. Bu kapsamda tüzük, üye devletlere, biyometrik bilgilerin işlenmesiyle ilgili olarak GDPR'nin çizdiği sınırı aşmamak ve temel hak ve özgürlüklere aykırı olmamak koşuluyla başka sınırlamalar getirme özgürlüğü tanımıştır.

GDPR temelli bir veri koruma uygulamasına sahip olan Birleşik Krallık cephesinde, Birleşik Krallık Veri Koruma Otoritesi (ICO - Information Commissioner's Office); İngiltere Gelir ve Gümrük İdaresi (HMRC – HM Revenue&Customs)'nin telefon destek hattını arayan kullanıcıların ses kaydı verilerinin işlenerek, otomatik bir ses tanıma (Voice ID) sistemi kurulmasıyla ilgili bir olayı incelemiş ve açık rıza alınmadan işlenen yaklaşık beş milyon kullanıcı verisinin silinmesi yönünde karar vermiştir [65]. Karara göre; rızası aranan kullanıcılara, bahse konu sistemden çıkma hakları olduğunun ve bu hakkı kullanmaları durumunda kendilerine sağlanan hizmetlerin olumsuz etkilenmeyeceğinin açıkça belirtilmesi gerektiği, sisteme dâhil olmanın mecburi olduğu yönünde bir izlenim uyandırmaktan da kaçınılması gerektiği belirtilmiştir.

Benzer şekilde İngiltere ve Galler Yüksek Mahkemesi, sivil haklar grubu Liberty tarafından getirilen bir adli inceleme soruşturmasında, Güney Galler Polisi (SWP - South Wales Police) ve Metropolitan Polis Servisi (MPS - Metropolitan Police Service) tarafından yürütülen bir yüz tanıma teknolojisinin (FRT – Face Recognition Technology) pilot planının, veri koruma mevzuatı da dâhil olmak üzere yasa ile tutarlı olup olmadığını değerlendirmiştir. ICO; kamusal alanlarda yüz tanıma teknolojisinin kullanımına ilişkin olarak "gizliliğe yönelik potansiyel tehdit" ve "insanların en hassas kişisel verileri" konusundaki endişelerini dile getiren bir açıklama yapmıştır. ICO, *"insanların yasal haklarını korumak için soruşturma ve icra gücünü kullanmaktan çekinmeyeceklerini"* söylemiştir [66].

Romanya Kişisel Veri İşleme Ulusal Denetleme Kurumu (ANSPDCP – Romanian National Supervisory Authority for Personal Data Processing), 2019 tarihinde, GDPR md. 7 uyarınca, *"Şirket, çalışanların biyometrik verilerini (parmak izlerini), veri gizliliği için daha az müdahaleci davranarak belirli odalara erişim için kullanabilir"* kararını vererek, genel veri işleme ilkelerine uymama ve "veri minimizasyonu ilkesinin ihlali" sebebiyle Entirely Shipping & Trading SRL şirketine 5.000 Euro (23.893 lei) para cezası vermiştir [67].

Bulgaristan Veri Koruma Komisyonu (KZLD - Data Protection Commision of Bulgaria) 2019 yılında, "*bilgi güvenliğinin korunmasını sağlamak için yetersiz teknik ve organizasyonel önlemler sonucunda, biyometrik veriler de dâhil olmak üzere, 33000'den fazla banka müşterisi ile ilgili 23000'den fazla veri kaydının sızdırılması*" sebebiyle, DSK Bankası'na 511000 Euro (1.000.000 BGN) para cezası vermiştir [68].

İsveç Veri Koruma Kurumu (Data Protection Authority of Sweden) 2019 tarihinde, Skellefteå Okulu'na *"öğrencilerin katılımını izlemek amacıyla veri işleme mümkün olsa da, yüz tanıma ile katılımın izlenmesinin amaçla orantısız olması, öğrenciler ve velilerinin, çocuklarının katılım amacıyla izlenmesini isteyip istemediklerine özgürce karar veremedikleri için rızanın uygulanamayacak olması, öğrencilerde kullanılan kamera gözetimi nedeniyle, hassas kişisel verileri işlemek için yeni teknoloji kullanılmasının yüksek riskli bir işleme faaliyeti olması"* sebepleriyle, 18630 Euro para cezası kesmiştir [69].

4.8.2. Kişisel Verilerin Korunması Kanunu (KVKK)

Ülkemizde 2016 yılında yürürlüğe giren 6698 sayılı KVKK, 95/46/AT sayılı direktif referans alınarak hazırlanmış olup, temelini Anayasa'nın 20. maddesi "Temel Hak ve Özgürlükler - Özel Hayatın Gizliliği"nden almaktadır. Söz konusu maddeye 2010 yılında eklenen fıkrayla birlikte, kişisel veriler üst düzenlemeyle birlikte koruma altına alınmıştır:

> "*Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebilir."*

Bununla birlikte, tüm temel hak ve özgürlüklerde olduğu gibi, kişisel verilere ilişkin koruma da mutlak değildir, diğer hak ve özgürlüklerde olduğu gibi sınırlanabilmektedir. Ancak bu sınırlamanın Anayasa'nın 13. maddesinde belirtilen esaslara uygun olarak gerçekleştirilmesi gerekmektedir:

> "*Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasa'nın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyet'in gereklerine ve ölçülülük ilkesine aykırı olamaz."*

Biyometrik veriler "*doğal bir kişinin fiziksel, fizyolojik veya davranışsal özellikleriyle ilgili özel teknik işlemlerden kaynaklanan kişisel verilerdir"* şeklinde tanımlanarak, KVKK md. 6/1 uyarınca "Özel Nitelikli Kişisel Veri" kapsamına alınmış olup, korunması daha sıkı şartlara bağlanmış ve ilgilinin açık rızası olmaksızın işlenmesi yasaklanmıştır. Bununla birlikte kanunlarda öngörülen hâllerde ve yeterli önlemler alınmak kaydıyla ilgili kişinin açık rızası aranmaksızın işlenebilmektedir.

Kişisel Verileri Koruma Kurulu'nun 2018/10 sayılı kararında [70], özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlarda güvenliğin sağlanması ile ilgili önlemler açıklanmıştır. Bu veriler eğer elektronik bir ortamda ise;

- Veriler kriptografik yöntemler kullanılarak muhafaza edilmeli,

- Kriptografik anahtarlar güvenli ve farklı ortamlarda tutulmalı,
- Verilerin bulunduğu ortamlara ait güvenlik güncellemeleri sürekli takip edilmeli, gerekli güvenlik testleri düzenli olarak yapılmalı/yaptırılmalı, test sonuçları kayıt altına alınmalı,
- Verilere bir yazılım aracılığıyla erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmeleri yapılmalı, bu yazılımların güvenlik testleri düzenli olarak yapılmalı/yaptırılmalı, test sonuçları kayıt altına alınmalı,
- Verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sistemi sağlanmalıdır.

Kurul, 2019/81 ve 2019/165 sayılı kararlarında [71] ise, spor salonu hizmeti sunan iki ayrı şirketin (veri sorumluları);

- üyelerinin giriş-çıkış kontrolünde el ve parmak izinin taranması suretiyle, kişilerin kimlik doğrulamasının yapılması hususunda özel nitelikli kişisel veri niteliğindeki biyometrik veri işleme faaliyetinde bulunulması,
- hizmetten faydalanmak için zorunlu ve tek yol olarak üyelere sunulması,
- üyelerin kulüplere girişlerde avuç içi bilgilerinin alınmasına rıza göstermemeleri hâlinde söz konusu hizmetten yararlanamayacakları ve kurala uyulmaması hâlinde firmaya fesih hakkı tanınmış olması,
- bu sebeple üyeler tarafından verilen açık rızaların özgür iradeye dayalı olduğunu söylemenin mümkün bulunmaması,
- kişisel verilerin işlenmesinde ölçülülük ilkesi ışığında ilgili kişilerden minimum düzeyde veri talep etme ilkesi ile uyumlu olarak kabul edilmemesi,
- bu bilgilerin güvenli şekilde muhafaza edildiğinden şüphe duyulması üzerine Kurul;
  - "*Spor Kulübünde giriş çıkış kontrolünün ve kulüp içerisindeki güvenliğin temini noktasında kulüp hizmetlerinden faydalanmak isteyen kişilere ilişkin giriş kontrollerinin biyometrik verileri işlemenin haricinde alternatif yollar ile sağlanması, biyometrik veri ile giriş çıkış işlemleri yapılmasının ve biyometrik veri işlemenin ivedilikle durdurulması hususunda veri sorumlularının talimatlandırılmasına;*

- *Veri sorumluları tarafından bugüne kadar işlenen ve muhafaza edilen el, parmak ve avuç izi ile ilgili verilerin Kanun'un 7. maddesi ile "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hâle Getirilmesi Hakkında Yönetmelik"* hükümlerine uygun olarak ivedilikle yok edilmesi, eğer ilgili özel nitelikli verilerin üçüncü kişilere aktarılması söz konusu ise, yok etmeye yönelik işlemlerin bu verilerin aktarıldığı üçüncü kişilere ivedilikle bildirilmesinin sağlanması hususunda veri sorumlularının talimatlandırılmasına,
- *Açık rızanın Kanun'un md 12/1-a'ya aykırılık teşkil etmesi nedeniyle Kanun'un md 18/1-b kapsamında idari para cezası uygulanmasına"* karar vermiştir.

Davalı idarenin, toptancı hâli biriminde görev yapan personelin mesai takibinin sağlanması amacıyla başlatılan yüz tarama sistemi uygulamasına son verilmesi talebi ile sendika tarafından açılan davanın, İstanbul 6. İdare Mahkemesince reddedilmesi sonucunda, davacı tarafından temyize başvurulduğu olayda; Danıştay 11. Dairesince "*Olayda, personelden kişisel veri alınması kapsamında olan "yüz tanıma sistemi" ile mesai takibi uygulamasının, kamusal alanda da olsa "özel hayatın gizliliği" ilkesi kapsamında bulunduğu açık olup, dava konusu işlem tarihi itibarıyla uygulamanın sınırlarını usul ve esaslarını gösteren bir yasal dayanağın bulunmaması, toplanan verilerin ileride başka bir şekilde kullanılamayacağına dair bir güvencenin mevcut olmaması göz önüne alındığında, Anayasa'nın "Temel Hak ve Hürriyetlerin Niteliği" başlıklı 12. maddesi ile "Özel Hayatın Gizliliği" başlıklı değişik 20. maddesi; Avrupa İnsan Hakları Sözleşmesinin "Özel Hayatın ve Aile Hayatının Korunması" başlıklı 8. maddesi ile Birleşmiş Milletler Medeni ve Siyasi Haklar Sözleşmesinin "Mahremiyet Hakkı" başlıklı 17. maddesi uyarınca, bahsi geçen temel haklar ve Anayasal ilkelerle bağdaşmayan dava konusu işlemde ve davanın reddi yolundaki mahkeme kararında hukuka uygunluk bulunmamaktadır."* şeklinde karara hükmederek, davacıyı haklı bulmuştur [72].

Davacının kimliğini ehliyet, nüfus cüzdanı ve öğretmen kimliği ile ispatlamasına ve Sosyal Güvenlik Kurumu (SGK) kapsamında sigortalı olduğunu tereddüde yer vermeyecek şekilde belgelemesine rağmen, avuç içini okutmadan verilecek sağlık hizmetlerinin SGK tarafından karşılanmayacağının bildirilmesi neticesinde açtığı davada, Danıştay 15. Dairesi 08.7.2014 tarihli ve 2014/1150 esas nolu kararında, 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu'nun 67. maddesinin 3. fıkrasında yer alan *"... Biyometrik*

yöntemlerle kimlik doğrulanması yapılması zorunludur" ibaresinin; "biyometrik yöntemlerle yapılacak kimlik doğrulaması sonucu elde edilecek kişisel verilerin toplanması ve işlenmesinin kapsamı ile, bu verilerin korunmasına ilişkin usul ve esasların belirtilmediği; bu nedenle, Yasama organı tarafından, temel ilkeleri konulmadan, çerçevesi çizilmeden biyometrik veri toplanmasına olanak veren biyometrik yöntemlerle kimlik doğrulamasının yapılmasının, Anayasa'nın 13. ve 20. maddelerine aykırı olduğu gibi, Anayasa'nın 2. maddesindeki hukuk devleti ilkesine de aykırı bulunduğu gerekçesine söz konusu kararda yer vermiştir [73].

Benzer şekilde verilmiş çok sayıda İdare Mahkemesi, Danıştay ve Avrupa İnsan Hakları Mahkemesi kararı olmakla birlikte, tam aksi kararlar da mevcuttur.

4.8.3. Türk Ceza Kanunu (TCK)

2004 tarihinde yürürlüğe giren 5237 sayılı TCK, özel olarak biyometrik verilerle ilgili düzenleme yapmış olmamakla birlikte, kişisel verilerin kaydedilmesi, hukuka aykırı olarak verilmesi/ele geçirilmesi ve verilerin yok edilmemesi konularında düzenlemeler içermektedir. Ayrıca suç konusu eylem, Anayasal hak olarak özel hayatın gizliliğini ihlal suçunun konusunu oluşturuyorsa, TCK md 134 kapsamında cezalandırılmaktadır.

Kişisel Verilerin Kaydedilmesi Madde 135- Hukuka aykırı olarak kişisel verileri kaydeden kimseye 1 yıldan 3 yıla kadar hapis cezası verilir.

Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Madde 136- Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, 2 yıldan 4 yıla kadar hapis cezası ile cezalandırılır. Suçun konusunun, kayda alınan beyan ve görüntüler olması durumunda verilecek ceza bir kat arttırılır.

Nitelikli Hâller Madde 137-Yukarıdaki maddelerde tanımlanan suçların;

a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle,

b) Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle, İşlenmesi hâlinde, verilecek ceza yarı oranında arttırılır.

Verileri Yok Etmeme Madde 138-Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde 1 yıldan 2 yıla kadar hapis cezası verilir. Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat arttırılır.

Şikâyet Madde 139- Kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ve verileri yok etmeme hariç, bu bölümde yer alan suçların soruşturulması ve kovuşturulması **şikâyete** bağlıdır.

Bu hükümler dışında, gerçekleştirilecek hukuka aykırı eylemler hırsızlık, dolandırıcılık gibi diğer suç tiplerinin işlenmesine sebep olduğu takdirde, söz konusu kanun hükümleri de işlerlik kazanacaktır.

4.9. SONUÇ VE DEĞERLENDİRMELER

Yıllardır güvenliği sağlamak için kullanılan kullanıcı adı/şifre ikilisinin yanı sıra, sürücü veya kimlik belgeleri ve güvenli binalara erişmek için kullanılan giriş kartları gibi belge tabanlı kimliklerin yerini biyometrik teknolojiler almaya başlamıştır. Kullanılan elektronik cihazlardan, ülke çapında yapılan işlemlere kadar birçok yerde kişiler, kimliklerini kanıtlamak için biyometrik sistemleri kullanmakta ve çok sayıda biyometrik veri üretmektedir. Hem daha pratik hem de daha güvenli olması sebebiyle de bu sistemler hızla yaygınlaşmaktadır. Ancak yapılan çalışmalar gösteriyor ki, biyometrik sistemler sızılamaz ve kırılamaz sistemler değildir. Bu bölümde sunulan tespitler doğrultusunda;

- biyometrik teknolojilerin kullanılması sonucunda çok sayıda verinin elde edildiği,
- toplanan biyometrik verilerden çok farklı alanlarda faydalanıldığı,
- toplanan verilerin ise elektronik ortamlarda saklanması, işlenmesi, taşınması veya kullanılması gibi durumlarda saldırılara açık olduğu,
- biyometrik verilerin hassas veriler olması sebebiyle, farklı menfaatler açısından değer kazanmaya başladıkları

açıklanmış;

- biyometrik sistemin çeşitli saldırılarla ele geçirilmesi dışında, yüz tanıma teknolojilerini maskeyle veya parmak izi tanıma teknolojilerini yapay silikon bir parmakla kandırılabildikleri

uzmanlarca kanıtlandığı belirtilmiştir.

Bu sistemlerin hâlihazırdaki kullanımı, gelecekteki gelişmeler ışığında daha geniş alanlara yayılarak birçok alana dâhil olacağını göstermektedir. Toplanan tüm biyometrik verilerin güvenliği, bireyden topluma, en sonunda devlete kadar uzanan güvenlik ihtiyacının temel taşını oluşturmaktadır. Bu sebeple gerek sistemlerin geliştirilmesi, gerek verilerin korunması, gerekse saldırılara karşı başarılı ve etkin önlemlerin alınması, üzerinde önemle ve istikrarla durulması gereken konular olmalıdır. Devlet kurumları ve şirketlerin farkındalığı ve iş birliği ile yürütülecek etkin bir sürece ihtiyaç zamanla daha da artacaktır.

Siber Güvenlik ve Adli Bilişim uzmanlarına başvuru kaynağı oluşturmak ve bu alanda çalışanları bilgilendirmek ve farkındalık yaratmak amacı ile hazırlanan bu çalışmada; önce Biyolojik Biyometrik Sistemler kapsamında değerlendirilen parmak izi, yüz, iris, retina, DNA, el geometrisi ve avuç içi tanıma gibi teknolojiler tanımlanarak, çalışma prensipleri anlatılmış, örnekler verilerek ve birbirleriyle olumlu/olumsuz yönleri karşılaştırılarak değerlendirmeler yapılmış, çalışmanın en sonunda da bu teknolojilerle ilgili uluslararası hukuki düzenlemeler anlatılarak, veri güvenliği ve KVKK ile ilişkisi irdelenmiştir.

Bu kapsamda bu çalışmada ayrıca, dünyada görülen saldırı, sahtekârlık ve güvenlik zafiyetlerinden örnekler verilerek, kişilere, kurumlara ve devletlere verilebilecek zararlardan bahsedilmiştir. Diğer taraftan, üretilecek donanımların fiziksel özelliklerindeki ihtiyaçlar da tespit edilen konular arasında yer almaktadır. Örneğin; bazı sistemlerde görülen fiziksel olarak fazla yer kaplama ve yüksek maliyet konuları, güvenlik konusunda sorun teşkil etmese bile, bu sistemlerin tercih edilmemelerine neden olmaktadır. Yüksek güvenlikli bölgelere erişim ve giriş çıkış kontrolü gereken noktalarda (havaalanı, teknik merkezler ve laboratuvar, banka, hastane, sınır kontrolü noktaları) kullanılan bu sistemlerin çalışması için gerekli donanımsal ekipmanlar çok fazla yer kaplamaktadır ve taşınabilir özelliğe sahip değildir [74].

Biyometrik teknolojinin kullanımı genişledikçe ve çeşitlendikçe, adalet kurumlarının, biyometrik bilgilerin toplanması, kullanımı, paylaşılması saklanması ve doğruluğu ile ilgili politikalarının gizlilik, sivil özgürlükler, medeni haklar ve bilgi kalitesi endişelerini dikkate alması sağlanmalıdır [75]. Zira biyometrik verilerin güvenliğini ve kullanımını sağlamak amacıyla, biyometrik veriler için özel olarak hazırlanmış yasalar bulunmamaktadır. Biyometrik veriler ülkemizde özel nitelikli kişisel veri kapsamında kabul edilip, kişisel

veriler ve kullanıcı gizliliği için yapılan düzenlemeler uyarınca işlenmektedir. Bu konuda daha özenli çalışmalar yapılması gerekmektedir.

Gelecekte yapay zekâ, makine öğrenmesi, mobil teknolojiler gibi alanların kullanımının genişlemesi ve yaygınlaşması ile ek donanım gerektirmeyen, daha kullanışlı, hızlı ve az masraflı, daha az yer kaplayan ve daha uygun boyutlarda, doğruluğu ve güvenirliliği daha yüksek ve çok daha güvenli sistemler geliştirilme potansiyeli yüksektir. Bu alanlarda çalışacak nitelikli uzmanların yetiştirilmesi ve biyometrik teknolojilerin geliştirilmesine yönlendirilmesi, saldırganlarla etkin mücadelede de olmazsa olmaz koşul olacaktır.

KAYNAKLAR

[1] NEC Global Safety Division, Biometrics: The State Of The Art in Public Safety. URL: https://www.nec.com/en/global/solutions/safety/pdf/NEC_Biometrics_Final.pdf, Son Erişim Tarihi: 09.06.2020.

[2] Muller, B. J. (2010). Security, Risk and the Biometric State: Governing Borders and Bodies. Publisher: Routledge, 1 edition, p. 162. Publication Date: 25.02.2010

[3] Garner, J. International Committee for Information Technology Standards (INCITS) Information Technology Industry Council (ITI). URL: https://www.standardsportal.org/usa_en/sdo/incits.aspx, Son Erişim Tarihi: 09.06.2020.

[4] International Organization for Standardization URL: https://www.iso.org/committee/45020.html, Son Erişim Tarihi: 09.06.2020.

[5] The History of Fingerprints, Why Fingerprint Identification? URL: https://onin.com/fp/fphistory.html, Son Erişim Tarihi: 09.06.2020.

[6] Neumann, C. (2012). Fingerprints at the Crime-Scene: Statistically Certain, or Probable? The Royal Statistical Society. URL: https://rss.onlinelibrary.wiley.com/doi/pdf/10.1111/j.1740-9713.2012.00539.x, Son Erişim Tarihi: 09.06.2020.

[7] Watson, S. How Fingerprinting Works. URL: https://science.howstuffworks.com/fingerprinting.htm, Son Erişim Tarihi: 09.06.2020.

[8] Crime Scene Forensics, LLC. (2018). History of Fingerprints. URL: http://www.crimescene-forensics.com/History_of_Fingerprints.html, Son Erişim Tarihi: 09.06.2020.

[9] The Crime Column. Fingerprint Analysis. URL: https://Thecrimecolumn.Com/Fingerprint-Analysis/, Son Erişim Tarihi: 09.06.2020.

[10] Mulawka, M. (2014). Postmortem Fingerprinting and Unidentified Human Remains. Forensic Studies for Criminal Justice. Publisher: Anderson; 1 edition, p. 132. Publication Date: 18.12.2013

[11] Kakıcı, A. (2008). Biyometrik Tanıma Sistemleri. URL: https://ahmetkakici.github.io/genel/biyometrik-tanima-sistemleri/, Son Erişim Tarihi: 09.06.2020.

[12] Harris, T. How Fingerprint Scanners Work. URL: https://computer.howstuffworks.com/fingerprint-scanner2.htm, Son Erişim Tarihi: 09.06.2020.

[13] Triggs, R. How Fingerprint Scanners Work: Optical, Capacitive, and Ultrasonic Variants Explained. URL: https://www.androidauthority.com/how-fingerprint-scanners-work-670934/, Yayım Tarihi: 28.03.2019. Son Erişim Tarihi: 09.06.2020.

[14] Shah, P. Ultrasonic Fingerprint Scanner vs Optical Fingerprint Scanner: How Do They Differ. URL: https://www.guidingtech.com/ultrasonic-fingerprint-scanner-vs-optical-fingerprint-scanner-how-do-they-differ/, Yayın Tarihi: 11.03.2019. Son Erişim Tarihi: 09.06.2020.

[15] 360 Biometrics. What are the different types of fingerprint sensors/readers? URL: https://www.360biometrics.com/faq/fingerprint_scanners.php, Son Erişim Tarihi: 09.06.2020.

[16] Şamlı, R., Yüksel, M. E. Biyometrik Güvenlik Sistemleri. XI. Akademik Bilişim Konferansı Bildirileri, Harran Üniversitesi, Şanlıurfa. 11-13 Şubat 2009.

[17] Bailenson, J. Detection of Comprehension & Emotion from Real-time Video Capture of Facial Expressions. Human Machine Interaction and Sensing. Stanford University's Virtual Human Interaction Lab. URL: https://mediax.stanford.edu/research-projects/hmi-bailenson/, Son Erişim Tarihi: 09.06.2020.

[18] Karakeçi, E. Yüz Tanıma Nedir? URL: https://erkankarakeci.wordpress.com/2011/12/16/yuz-tanima-nedir/, Yayın Tarihi: 16.12.2011. Son Erişim Tarihi: 09.06.2020.

[19] Musayeva, G., Yahyayev, M. (2014). Biyometrik Güvenlik Sistemleri. İstanbul Aydın Üniversitesi. URL: https://www.researchgate.net/publication/271210599_Biyometrik_Guvenlik, Son Erişim Tarihi: 09.06.2020.

[20] The University of Southampton. Chapter 13- Face recognition 101: Eigenfaces. URL: http://openimaj.org/tutorial/eigenfaces.html, Son Yayım Tarihi: 09.02.2020. Son Erişim Tarihi: 09.06.2020.

[21] Eigen Faces and A Simple Face Detector with PCA/SVD in Python URL: https://sandipanweb.wordpress.com/2018/01/06/eigenfaces-and-a-simple-face-detector-with-pca-svd-in-python/, Yayım Tarihi: 06.01.2018. Son Erişim Tarihi: 09.06.2020.

[22] Anggo, M., La Arapu. (2018). Face Recognition Using Fisherface Method. Journal of Physics Conference Series 1028 (1): 012119. DOI: 10.1088/1742-6596/1028/1/012119

[23] Face Recognition Using Fisherfaces. URL: https://iq.opengenus.org/face-recognition-using-fisherfaces/, Son Erişim Tarihi: 09.06.2020.

[24] Xu, Yajun., Liang, Fengmei., Zhang, Gang., Xu, Huifang. (2016). Image Intelligent Detection Based on the Gabor Wavelet and the Neural Network. Symmetry Journal 8 (11): 130. DOI: 10.3390/sym8110130

[25] Jurafsky, D., Martin, J. H. (2019). Hidden Markov Models. Speech and Language Processing. URL: https://web.stanford.edu/~jurafsky/slp3/A.pdf, Son Erişim Tarihi: 09.06.2020.

[26] Hameed R. F., Mahmuod H. Al-Muifraje, Thamir R. S. (2019). Face Recognition System Based on Continuous One-State Model. AIP Conference Proceedings 2144, 050001. URL: https://aip.scitation.org/doi/10.1063/1.5123117, Son Erişim Tarihi: 09.06.2020.

[27] Samaria, F., Fallside, F. (1993). Face Identification and Feature Extraction Using Hidden Markov Models. Image Processing: Theory and Applications, Elsevier, pp 295–298, 199.

[28] Chengjun Liu, Wechsler, H. (1998). Face Recognition Using Evolutionary Pursuit. European Conference on Computer Vision, pp 596-612. URL: https://link.springer.com/chapter/10.1007/BFb0054767, Son Erişim Tarihi: 17.012.2020.

[29] Tisse, C., Martin, L., Torres, L., Robert, M. Person Identification Technique Using Human Iris Recognition. Proceedings of 15th International Conference on Vision Interface, Calgary. pp. 294-299. 27-29 May 2002.

[30] Galeano, D. (2012). Identity enciphered in the body: The bertillonnage and the Anthropometric Office in the Police of Rio de Janeiro, 1894-1903. Boletimdo Museu Paraense Emilio Goeldi: Ciencias Humanas 7 (3): 721-742. DOI: 10.1590/S1981-81222012000300007

[31] Çakır, A., Altıntaş, V., Akbulut, F. T. (2013). İris Tanıma Sistemleri ve Uygulama Alanları. Akademik Bilişim 2013 – XV. Akademik Bilişim Konferansı Bildirileri. 23-25 Ocak 2013 – Akdeniz Üniversitesi, Antalya

[32] Daugman, J. (1992). High Confidence Personal Identification By Rapid Video Analysis of Irıs Texture. IEEE Proc. International Carnahan Conference on Security Technology: Crime Countermeasures. Atlanta, GA, USA. 14-16 Oct. 1992. DOI: 10.1109/CCST.1992.253755

[33] Dandıl, E., Kaplan, K. İ. Biyometrik İris Sınıflandırma Sistemleri. XV. Akademik Bilişim Konferansı Bildirileri. Akdeniz Üniversitesi, Antalya. 23-25 Ocak 2013.

[34] Pourreza, H. R., Azizi, A. (2009). A Novel Method Using Contourlet to Extract Features for Iris Recognition System. Emerging Intelligent Computing Technology and Applications. pp. 544-554. DOI: 10.1007/978-3-642-04070-2_60

[35] Aslam, T. M., Tan, S.Z., Dhillon, B. (2009). Iris Recognition in The Presence of Ocular Disease. Journal of The Royal Society Interface, vol. 6, no. 34, pp. 489-93. DOİ: 10.1098/rsif.2008.0530

[36] The Electronic Frontier Foundation. Iris Recognition. URL: https://www.eff.org/tr/pages/iris-recognition, Son Güncelleme Tarihi: 25.10.2019. Son Erişim Tarihi: 09.06.2020.

[37] Koç, H. K. (2019). Biyometrik Tanı Yöntemlerinde Kişisel Veri Güvenliği Arttırılmış Sistem Tasarımı. Mersin Üniversitesi Yüksek Lisans Tezi.

[38] Gold, S. Iris Biometrics: A Legal Invasion of Privacy? Biometric Technology Today. Volume 2013, Issue 3, pp. 5-8. Pages 5-8 March 2013. URL: https://doi.org/10.1016/S0969-4765(13)70053-5.

[39] Das, R. Retinal Recognition – The Ultimate Biometric. Infosec Institute. URL: https://resources.infosecinstitute.com/retinal-recognition-ultimate-biometric/#gref, Son Erişim Tarihi: 09.06.2020.

[40] Yalçın, N., Gürbüz, F. (2015). Biyometrik Güvenlik Sistemlerinin İncelenmesi, Düzce Üniversitesi Bilim ve Teknoloji Dergisi,3. pp. 398-413. URL: http://static.dergipark.org.tr/article-download/imported/5000094331/5000120481.pdf?, Son Erişim Tarihi: 09.06.2020.

[41] Venngage. DNA Fingerprinting to Determine Paternity. URL: https://infograph.venngage.com/p/219962/dna-fingerprinting-to-determine-paternity-infographic, Son Erişim Tarihi: 09.06.2020.

[42] Soltysiak, S.,Valizadegan, H. (2008). DNA as a Biometric Identifier. Computer Science and Engineering Department, Michigan State University .

[43] Inderscience Publishers. (2008). Handheld DNA Detector. Science Daily. URL: http://www.sciencedaily.com/releases/2008/03/080310173246.htm, Son Erişim Tarihi: 09.06.2020.

[44] Mayhew, S. Explainer: Hand Geometry Recognition. Biometric Update URL: https://www.biometricupdate.com/201206/explainer-hand-geometry-recognition, Yayın Tarihi: 25.06.2012. Son Erişim Tarihi: 09.06.2020.

[45] Jain, A. K., Ross, A., Pankanti, S. A. (1999). Prototype Hand Geometry Based Verification System. Appeared in Proc. of 2nd Int'l Conference on Audio- and Video-based Biometric Person Authentication (AVBPA). pp. 166-171, Washington D.C. March 22-24.

[46] Md. Khaliluzzaman, Md Mahiuddin; Md. Monirul İslam. (2018). Hand Geometry Based Person Verification System. International Conference on Innovations in Science, Engineering and Technology (ICISET). Chittagong, Bangladesh. 27-28 Oct. 2018. DOI: 10.1109/ICISET.2018.8745620

[47] GiTae Park, Soowon Kim. (2013). Hand Biometric Recognition Based on Fused Hand Geometry and VascularPatterns. 13 (3): 2895–2910. DOI: 10.3390/s130302895

[48] National Science and Technology Council Committee on Homeland and National Security, Subcommittee on Biometrics. Hand Geometry. pp 110-113. URL: https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence/files/hand-geometry.pdf, Son Erişim Tarihi: 09.06.2020.

[49] Önen Yıldız, H. G. (2010). Avuçiçi Esaslı Biyometrik Kimlik Tanımlama ve Doğrulama. Marmara Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi. İstanbul.

[50] Michael, G. K., Connie, T. ve Beng Jin T. A. A Contactless Biometric System Using Palm Print and Palm Vein Features. DOI: 10.5772/19337, Yayın Tarihi: 09.08.2011.

[51] Charfi, N. (2017). Biometric Recognition Based on Handschape and Palmprint Modalities. Ecole nationale supérieure Mines-Télécom Atlantique. Le département Image et Traitement de l'Information. l'Université Bretagne Loire. p. 178. URL: https://tel.archives-ouvertes.fr/tel-01781354/document, Son Erişim Tarihi: 09.06.2020

[52] Alçın, M. (2009). Görüntü İşleme Esaslı Parmakizi Doğrulama. Marmara Üniversitesi, Elektronik-Bilgisayar Anabilim Dalı, Yüksek Lisans Tezi.

[53] Ergen, B., Çalışkan, A. (2011). Biyometrik Sistemler ve El Tabanlı Biyometrik Tanıma Karakteristikleri, 6th International Advanced Technologies Symposium (IATS'11). URL: http://web.firat.edu.tr/iats/cd/subjects/Electrical%26Electronics/EAE-94.pdf, Son Erişim Tarihi: 10.06.2020.

[54] Putte, T., Keuning, J. (2000). Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned. Smart Card Research and Advanced Applications: IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications. Bristol, United Kingdom. pp. 289-306. 20–22 September 2000.

[55] S. Liu, Silverman, M. (2011). A Practical Guide to Biometric Security Technology. IT Professional, vol. 3, no. 1, pp. 27–32.

[56] Jain, A. K., Bolle, R., Pankanti, S. (1999). Biometrics: Personal Identification in Networked Society. Springer Science & Business Media. P. 411. DOI: 10.1007/978-0-387-32659-7

[57] Unar, J., Senga, W., Abbasia, A. (2014). A Review of Biometric Technology Along with Trends and Prospects. Pattern Recognition, vol.47, pp. 2673 – 2688.

[58] Diaz, V. Legal Challenges of Biometric Immigration Control Systems. Mexican Law Review. Volume 7, Issue 1, Pages 3-30. July–December 2014. DOI: 10.1016/S1870-0578(16)30006-3

[59] Thakkar, D. Bıometrıc Data Securıty: How Different Techniques are Leveraged to Secure Biometric Data. URL: https://www.bayometric.com/techniques-secure-biometric-data/, Son Erişim Tarihi:10.06.2020.

[60] Bontrager, P., Roy, A., Togelius, J. (2018). DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution. Appeared in Proceedings of IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS). Los Angeles, USA. DOI: 10.1109/BTAS.2018.8698539

[61] Yu Chen , Bin Ma, Zhuo Ma. (2019) USA Black Hat Conference. August 3-8, *2019*. Mandalay Bay/Las Vegas.

[62] Westerlund, M. (2019). The Emergence of Deepfake Technology: A Review. Technology Innovation Management Review 9 (11): 39-52. November 2019. DOI: 10.22215/timreview/1282

[63] Küzeci, E. (2010). Kişisel Verilerin Korunması. Turhan Kitabevi, 3. Baskı, p. 564. Ankara.

[64] Wernick, A. S. Biometric Information – Permanent Personally Identifiable Information Risk. The American Bar Association – ABA URL: https://www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_8/, Yayın Tarihi: 14.02.2019. Son Erişim Tarihi: 10.06.2020.

[65] Information Commissioner's Office - ICO 03.05.2019 URL:https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/05/ico-says-that-voice-data-collected-unlawfully-by-hmrc-should-be-deleted/ Son Erişim Tarihi: 17.12.2020

[66] Information Commissioner's Office. ICO Investigation Into How the Police Use Facial Recognition Technology in Public Places. 31.10.2019. URL: https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf Son Erişim Tarihi: 17.12.2020

[67] Romanya Kişisel Veri İşleme Ulusal Denetim Otoritesi (ANSPDCP - Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal)'nin 13.12.2019 Tarihli Kararı. URL: https://www.dataprotection.ro/?page=O_noua_sanctiune_pentru_incalcarea_RGPD_2020_3&lang=ro, Son Erişim Tarihi: 10.06.2020.

[68] Bulgaristan Veri Koruma Komisyonu (KZLD - Data Protection Commision of Bulgaria)'nun 28.08.2019 Tarihli Kararı. URL: https://www.cpdp.bg/index.php?p=news_view&aid=1514, Son Erişim Tarihi: 10.06.2020.

[69] İsveç Veri Koruma Kurumu (Data Protection Authority of Sweden)'nun 20.08.2019 Tarihli Kararı. URL: https://www.datainspektionen.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf, Son Erişim Tarihi: 10.06.2020.

[70] Kişisel Verileri Koruma Kurumu 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı. URL: https://www.kvkk.gov.tr/Icerik/4110/2018-10, Son Erişim Tarihi: 10.06.2020.

[71] Kişisel Verileri Koruma Kurumu 25/03/2019 Tarihli ve 2019/81 Sayılı Karar ve 31/05/2019 Tarihli ve 2019/165 sayılı Karar. URL: https://www.kvkk.gov.tr/Icerik/5496/2019-81-165, Son Erişim Tarihi: 10.06.2020.

[72] Danıştay 11. Daire E. 2017/816, K. 2017/4906, T. 13.06.2017

[73] Akgül, A. (2015). Kişisel Verilerin Korunması Bağlamında Biyometrik Yöntemlerin Kullanımı ve Danıştay Yaklaşımı. Türkiye Barolar Birliği Dergisi. URL: http://tbbdergisi.barobirlik.org.tr/m2015-118-1477, Son Erişim Tarihi: 10.06.2020.

[74] Arslan, B., Sağıroğlu, Ş. (2016). Mobil Cihazlarda Biyometrik Sistemler Üzerine Bir İnceleme. Politeknik Dergisi. cilt 19 , sayı 2, Sayfalar 101 – 114. URL: https://dergipark.org.tr/tr/pub/politeknik/issue/33079/368083, Yayın Tarihi: 01.06.2016. Son Erişim Tarihi: 10.06.2020.

[75] U.S. Department of Justice's Global Justice Information Sharing Initiative – Privacy and Information Quality Risks: Justice Agency Use of Biometrics. URL: https://it.ojp.gov/documents/d/biometrics%20flyer_v2.pdf, Son Erişim Tarihi: 10.06.2020.

Bölüm 5

DAVRANIŞSAL BİYOMETRİK SİSTEMLER, TEKNOLOJİLER VE GÜVENLİK

Hande Tutumluer - Refik Samet

Bilgi çağı ile birlikte siber suçların çeşitleri ve önemi her geçen gün artmaktadır. Bu koşullara bağlı olarak, güvenlik ihtiyacı bugün en üst düzeydedir. Hemen her kuruluş birçok kişinin hassas verilerini veri tabanlarında saklamaktadır ve bu verilerin güvenliğinden sorumludur. Bilgi güvenliğinin temelinin gizlilik, bütünlük ve kullanılabilirlik (CIA Triad) ilkelerine dayandığı göz önünde bulundurulduğunda, verilerin yetkisiz erişime karşı sıkıca korunması gerekmektedir. Güvenliği arttırmanın yollarından biri de kişiyi tanımlamak veya doğrulayabilmektir. Kişiyi tanımlamak ve doğrulamak amacıyla biyometrik sistemler kullanılmaktadır.

Biyometrik sistemler, temel olarak Biyolojik ve Davranışsal olarak ikiye ayrılmaktadır. Biyolojik Biyometrik Sistemler; yüz, parmak izi, el, iris, retina, DNA, ses, koku gibi biyolojik teknolojilerle tanımlanırken, Davranışsal Biyometrik Sistemler; metin ve e-posta yazarlığı, eskiz çizimi ve boyama stili, klavye tuş vuruşları ve fare dinamikleri, komut satırı girdileri ve grafiksel kullanıcı ara yüzü kullanımı, gülümseme ve dudak hareketleri, bakışlar ve göz hareketleri, yürüyüş, haptik cihaz kullanımı, imza ve el yazısı, ses ve konuşma stili, araba sürüş stili, oyun stratejileri, kredi kartı kullanım alışkanlıkları ve programlama stili gibi davranışsal teknolojilerden oluşmaktadır. "Davranışsal Biyometrik Sistemler, Teknolojiler ve Güvenlik" konulu bu bölümün amacı, davranışsal biyometrik sistemlerin özellikleri, bu sistemlerde kullanılan teknolojilerin çeşitleri, bu sistemlerin güvenlik amacıyla kullanım yöntemleri ve biyometrik verilerle ilgili kanuni düzenlemeler gözden geçirilmiş ve konu ile ilgili değerlendirmeler sunulmuştur.

5.1. GİRİŞ

Günümüz teknolojilerine uygun olarak bir kişinin kimliğini ispat edebilmek için üç yaklaşım bulunmaktadır [1].

***Bilgi faktörü (something you know)*:** Parola, PIN kodu, kullanıcı adı, kimlik numarası, güvenlik sorularının cevapları vb. parolalar en yaygın kimlik doğrulama yöntemi olmasına karşın aynı zamanda kırılması en kolay olan yöntemdir. Tahmin edilebilir, unutulabilir ve paylaşıma açıktır, bu nedenle ikinci bir güvenlik katmanına ihtiyaç duyulmuştur.

Sahip olma faktörü (something you have): Smart kart, token, telefon, dongle, anahtar vb. İkinci faktör güvenlik elemanları ise kaybolma ve çalınma gibi riskler taşıdığından kullanıcının fiziksel olarak da içinde bulunduğu yeni bir güvenlik katmanı geliştirilmiştir.

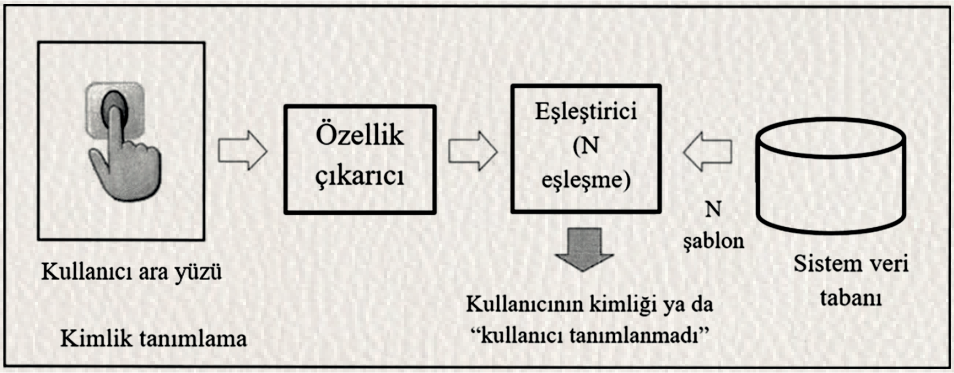
Biyometri (something you are): Parmak izi, yüz, ses, iris vb. Gelişmiş araçlar olmadan biyometriler çalınamaz, değiştirilemez ve kaybedilemez. Bu yaklaşımların kombinasyonu sistemi oldukça güvenli hâle getirmektedir.

Güvenliğin gücü en zayıf halkası ile ölçüldüğünden bu yaklaşımların kullanılması son derece önemlidir. Bir ev için üç faktörlü doğrulama (Şekil 5.1) aşırı iken, verilerin güvenliğinin büyük önemi olduğu bir banka ya da Ar-Ge binası için doğru bir tercih olacaktır.

Şekil 5.1. Üç faktörlü doğrulama yapısı [2]

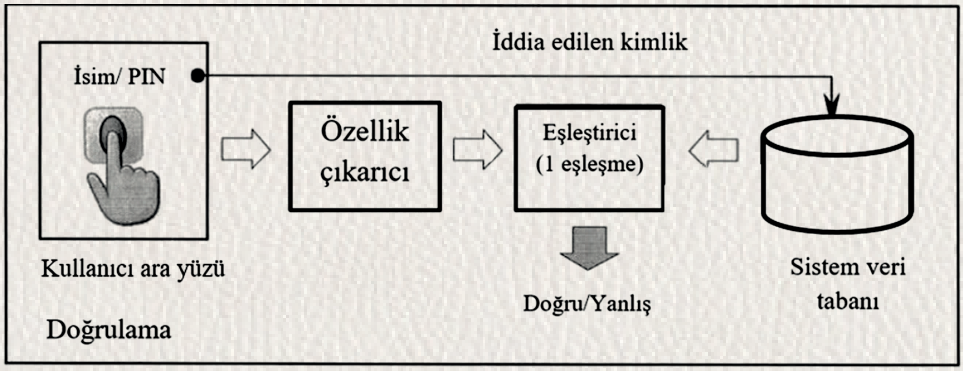
Biyometriler kişinin kendine özgü verileriyle kimliğinin tanımlanmasını ve doğrulanmasını sağlar. Bu işlemler aslında sırasıyla "Siz kimsiniz?" ve "Siz gerçekten iddia ettiğiniz kişi misiniz?" sorularını cevaplamaktır.

- **Kimlik Tanımlama:** Kayıtlı kimliklerin bulunduğu bir veri tabanından istenen kişinin doğru kimliğinin seçilmesidir. Kişiye ait biyometri ile veri tabanında depolanan tüm biyometrik şablonlar arasında bir karşılaştırma yapılır ve sistem ya "en iyi" eşleşmeyi yapar ya da olası eşleşmeleri puanlar ve benzerliklerine göre sıralar [3]. Şekil 5.2'de kimlik tanımlanmasına ait bir örnek verilmiştir.



Şekil 5.2. Kimlik tanımlama [3]

- **Kimlik Doğrulama:** Bir kişinin iddia ettiği kişi olup olmadığının sorgulanmasıdır. Kişiye ait biyometri ile veri tabanında bulunan belirli bir şablon arasında bir karşılaştırma yapılır, birebir eşleşme doğru ise kimlik doğrulanmış olur [4]. Şekil 5.3'te kimlik doğrulamaya ait örnek verilmiştir.



Şekil 5.3. Kimlik doğrulama [4]

İnsanlar günlük işlerini yerine getirirken farklı yöntemler kullanır, bu da onlara farklı davranış stilleri kazandırır, bu davranış biçimleri kişiye özgüdür. Davranış biyometrisi araştırmacıları sergilenen bu davranışsal özellikleri ölçmeye çalışır ve bu ölçümlerle kimlik doğrulaması yapmak hedeflenir. Ölçüm sonucu elde edilen bu biyometrik verilerle o kişiye ait davranış profili çıkarılır. Profil hazırlandıktan sonra kimliği sürekli olarak doğrulamak için hareketler sessizce izlenir. Profille eşleşmeyen alışılmadık davranış kalıpları gözlendiğinde tercihe göre sistem diğer kimlik doğrulama formlarını talep edebilir, kullanıcı erişimini engelleyebilir, cihazı dondurabilir veya kendini kapatabilir.

Davranış biyometrileri mors kodlarındaki kalıpların doğrulandığı 19. yy'dan beri hayatımızda yer almaktadır. Bugün en çok incelenen özellikler arasında yürüme biçimi ve siluet, konuşma sesi, imza, el yazısı ve tuş vuruşları/yazma ritmi ve dokunmatik dinamiklerini sayabiliriz [5].

Toplanan verilere göre davranışsal biyometriyi dört başlıkta incelenebilir;

1. Kaynak Tabanlı Davranışsal Biyometri
2. İnsan- Bilgisayar Etkileşimi Tabanlı Davranışsal Biyometri
3. Motor Beceriye Dayalı Davranışsal Biyometri
4. Saf Davranışsal Biyometri

5.2. KAYNAK TABANLI DAVRANIŞSAL BİYOMETRİ

Kaynak tabanlı davranışsal biyometri; kullanıcı tarafından üretilen çizim/eskiz, resim ya da metni incelemeye yarayan biyometrilerdir. Kişinin kelime dağarcığı, resimdeki renk ve ton skalası, anlatımda seçilen kelimeler veya kullanılan noktalama işaretleri eser sahibine ait taklidi zor bir stil ortaya çıkarır.

Kaynak tabanlı davranışsal biyometri çeşitleri:

- Metin yazarlığı,
- E-posta yazarlığı,
- Eskiz stili,
- Boyama stili.

5.2.1. Metin Yazarlığı

Yazılı metinler dilbilgisi ve üslup açısından analiz edilebilmektedir. Bu analiz için profil oluşturulurken; söz kalıpları, söz dizimi, cümle ve kelime sayısı, noktalama işareti sayısı, bilgi içeriği, deyim ve atasözleri, edatlar, anlambilim, alıntılar gibi özellikler göz önünde bulundurulur.

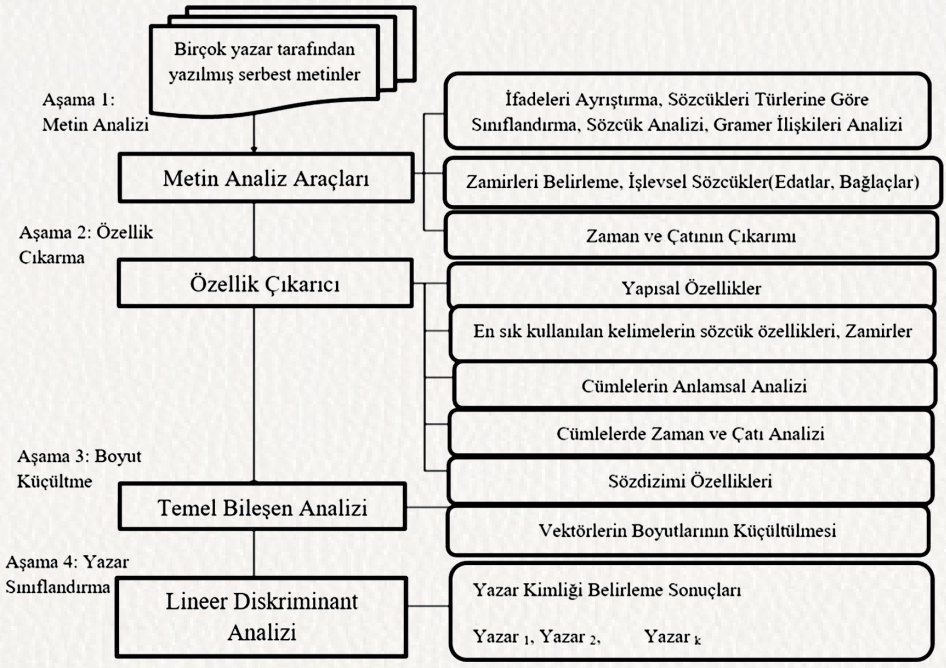
Dilbilimsel profil oluşturmayı konu edinen bir araştırma, yazar kimliği tanımlama ve doğrulama için kesinlikle değerini göstermiştir. Söz dizimi özelliklerin kombinasyonunu kullanan bir profil oluşturma sisteminin, test grubundaki metinlerin %97'si için doğru yazarı seçebildiği kaydedilmiştir [6].

Büyük bir anonim metin verildiğinde yazar doğrulamasının nasıl yapılacağının araştırıldığı bir çalışmada metin kategorizasyon yöntemleri uygulanmıştır [7]. Metinler temizlenmiş ve aynı anlama gelen kelimeler birleştirilmiş, en sık kullanılan 200 kelime belirlenerek vektör oluşturulmuştur.

Yazar doğrulama, metin ile yazar ilişkilendirmeden çok daha zordur bu nedenle araştırmacılar, bir yazarın tarzındaki bilinçli veya bilinçsiz değişiklikleri yansıtan nispeten sığ farklılıkları ve farklı yazarların tarzlarını yansıtan daha derin farklılıkları ayırt etmeyi öğrenmelidir [8].

Metin yazarlığı profillemesi ile yazarların kimliği doğrulanmış eserleri kullanılarak sahte yazarların maskeleri düşürülebilir, anonim kalmış eserlerin gerçek sahipleri bulunabilir. Şekil 5.4'te metin yazarlığı davranışsal biyometri çeşidine ait örnek verilmiştir.

Kime ait olduğu bilinmeyen yazılı eserler üzerinde çalışılırken ilk aşamada eser içeriği incelenir. Anlam ve yapı yönünden analiz edilen metnin 2. aşamada biyometrik veri olarak kullanılabilecek dilbilgisi özellikleri çıkarılır. 2. aşama sonunda her belge bir vektöre sahiptir. Daha teknik bir evre olan 3. aşamada bu özellikler yardımıyla hazırlanan vektörler küçültülür ve 4. aşamada ise yapılan hesaplamalar doğrultusunda yazarlar belirlenir.



Şekil 5.4. Metin yazarlığı tanımlama algoritması [9]

5.2.2. E-posta Yazarlığı

İnsanların e-posta gönderme alışkanlıkları birbirinden oldukça farklıdır. E-posta yazarlığı içerik yönünden metin yazarlığına benzese de, posta gönderim ve alım verileri analiz edilerek ayrıntılı bir profil oluşturabilir. Temel amaç yazar tarafından yazılan e-postalardan sabit bir dizi özellik elde ederek büyük yığınlar arasında yazarın kimliğini belirleyebilmektir.

Profilleme yardımıyla alışılmadık adreslere e-posta gönderilmesi gibi anormal davranışlar gözlemlenerek virüs yayılımı tespit edilmesi üzerine araştırmalar yapılmıştır [10]. E-postanın uzunluğu, e-postanın gönderilme saati, e-posta erişiminin masaüstü/tablet bilgisayarlarla ya da mobil telefonla sağlanması, gelen ve çöp kutusunun boşaltılma sıklığı, alıcıların e-posta adresleri, e-posta ile gönderilen ekler, resmî e-postalarda kullanılan dil ve üslup, selamlama ve imza gibi yaklaşık 200 değişken yardımıyla oldukça başarılı sonuçlar alınmaktadır.

Adli soruşturmalara yardım etmek amacıyla e-posta yazar kimliğini tespit etmek üzere yapılan bir çalışmada ise e-posta içerik madenciliği teknikleri kullanılmıştır. Farklı yazarlar tarafından oluşturulan dokümanlarla destek vektör makinesi öğrenme algoritması uygulanmış ve başarılı sonuçlar alınmıştır [11].

E-posta yazarlığı biyometrilerinin kullanımı yaşanan dijital dönem göz önünde bulundurulduğunda adli soruşturmalar için faydalı olacaktır. İzi sürülen e-postalar yazarları ile eşleştirilebilir, yazarlar arasında yüksek hassasiyetle bir ayrım yapılamasa da belirli yazım hataları ve üslup farklılıkları küçük bir örneklemde başarılı sonuçlar verecektir.

5.2.3. Eskiz Stili

Bir kişinin dikkatini vermeden ya da dalgınlıkla çizdiği şekillere karalama (doodle) denir ve bu çizimler de el yazıları kadar benzersiz olduğundan eskiz/karalama stili kaynak tabanlı davranış biyometrileri arasındadır.

Karalama biyometrisi ile doğrulamanın araştırıldığı bir çalışmada deneklerin çizdiği şekillerin (doodle) konumuna, çizim hızlarına ve çizim sürelerine göre profil oluşturulmuştur. Kullanıcıların parolalarını sisteme öğretmesinin ardından parolalar ekranlara çizilerek doğrulama yapılır [12].

Basit geometrik şekiller çizdirerek kimlik doğrulaması yapan bir başka çalışmada ise, şekilleri birleştirmek için pek çok kombinasyon bulunduğundan yeterince güvenilir bulunmuştur. Şekillerin karmaşıklığını arttırma, ek şekiller çizdirerek aralarında bağlantı kurulmasını isteme gibi yöntemlerle sistemin performansı iyileştirilebilir [13].

5.2.4. Boyama Stili

Bugün bir dergide, müzede ya da İnternet'te karşımıza çıkan tabloların hangi ressama ait olduğu konusunda tahmin yürütülebiliyorsa, bu ressamın boyama stili hakkında bilgi sahibi olunduğundandır. Nilüferlerden Monet'i, ayçiçeklerinden Van Gogh'u hatırlamak profillemeye bir örnektir.

Sanat eserleri üzerinde yapılan bir çalışmada, yazılı eserlerin üsluplarına göre yazar doğrulaması yapılması gibi resimlerin boyama stilleri incelenerek sanatçı kimliği doğrulaması yapılmaya çalışılmıştır. Çalışmada Pieter Bruegel the Elder'a atfedilen 13 resimlik bir koleksiyonun kimlik doğrulama sorunu

ve Rönesans ressamı Pietro Perugino'nun bir portresinin çizerleri ele alınmıştır. Brugel'in sekiz adet kimliği doğrulanmış eseri ile beş adet taklidi dijital olarak taranarak istatistiksel özellikleri çıkarılmış, gerçek eserlerle taklitler arasındaki bariz fark ortaya konmuştur. Perugino portresi analizinde ise resim geniş formatlı bir fotoğraf makinesi ile fotoğraflanmış ve bu görüntü gri tonlamaya dönüştürülmüştür. Resimdeki altı karakterin yüzleri arasındaki istatistiksel farklılıkların ışığında resimde en az 4 kişinin çalıştığı, muhtemelen Perugino'nun resmin sadece bir kısmını boyadığı gerisini çıraklarının tamamladığı tespit edilmiştir [14].

Sanat eserlerinde sahtecilik sanat tarihi kadar eskidir. Sahteciliğin önünü kesmek için bugün x-ray ışınları ve deneyimli sanat tarihçilerinin tecrübeleri ile sanat eserleri korunmaya çalışılıyor. Doğrulanmış eserlerin boyama biyometrileri baz alınarak hazırlanan istatistiksel profiller sayesinde yanlış ressamlara atfedilen eserler gerçek kimliklerine kavuşabilir, bilinen bir tabloya katkı yapan diğer sanatçıların sayısı tespit edilebilir.

5.3. İNSAN - BİLGİSAYAR ETKİLEŞİMİ TABANLI DAVRANIŞSAL BİYOMETRİ

İnsanlar günlük hayatta bilgisayarlarını ve diğer akıllı cihazlarını kullanırken farkında olmadan kendilerine özgü bir stil geliştirirler. Bu özellikleri ölçmek ve kimlik doğrulama için kullanabilme amacıyla klavye ve fareyle etkileşimde bulunan kasların hareketleri, bilgisayar yazılımının gözlemlenebilir eylemleri üzerinden kullanıcının davranışını izleyerek elde edilir. Bu kategori insan-bilgisayar etkileşimini sadece doğrudan değil, dolaylı yoldan da incelemektedir. Bilgisayarda bulunan kayıt günlükleri, program ekle/kaldır geçmişi ve sisteme ait diğer kayıtlar da profil özelliklerine eklenebilir. Donanımsal ve yazılımsal veriler bu kategorinin alanıdır.

İnsan-bilgisayar etkileşimi tabanlı biyometri çeşitleri:

- Tuş vuruşu dinamikleri,
- Fare dinamiği,
- Komut satırı girdileri,
- Grafiksel kullanıcı ara yüzü.

5.3.1. Tuş Vuruşu Dinamikleri

Klavye ile yazı yazmak her kişi için karakteristik özellikler taşır. Deneyimli bir kullanıcı ile ilk kez klavye kullanan bir kişinin yazı kalıpları aynı olmaz. Bu farklılıklar göz önünde bulundurularak kişiye özel yazı (davranış) kalıpları oluşturulup kimlik doğrulaması yapılabilmektedir. Kimlik doğrulaması için, kullanıcı adı ve şifresi girişi gibi basit bir yazma örneği yeterlidir ancak kullanıcı tanımlama için büyük miktarda tuş vuruşu verisine ihtiyaç vardır ve tanımlama, sistemde bulunan diğer tüm kullanıcıların profilleri ile yapılan karşılaştırmalara dayanır [15,16].

Profil oluşturulurken; tuş vuruş hızı, genel yazma hızı, tuşlar arası bekleme süresi, bir tuşa basılan süre, sayısal tuş takımının kullanımı, yazım hatalarının sıklığı (geri al ve silme), tuş seçimi (ctrl, shift, enter tuşlarından iki tane bulunmaktadır.) özelliklerinden faydalanılır.

Tuş vuruşu dinamikleri analizi ile yapılan çalışmalar yazım örnekleri farklı dillerde yazıldığında bile kullanıcı tanımlama ve kimlik doğrulaması için kullanılabileceğini göstermiştir. Kimlik belirlemenin öneminin arttığı kritik noktalarda, insanların farklı dilleri konuştuğu uluslararası alanlarda bile başarılı sonuçlar veren tuş vuruşu analizinin öneminin altı çizilmiştir [17].

Klavye dinamikleri 1980'den beri kimlik doğrulama yöntemi olarak araştırılmaktadır. Bekletme süreleri, tuş vuruşları arasında geçen zaman gibi özelliklerin de deneylere dâhil edilmesiyle kimlik doğrulamada %1'in altında false negative oranı alınmıştır. Çalışmalar klavye kullanımının da bir "imza" niteliği taşıdığını vurgulamıştır [18].

Kullanıcının tuş vuruşu istatistiklerini ele geçiren bilgisayar korsanları bir davranış profili oluşturabilmektedirler. Profili ele geçirilen bir kullanıcı İnternet ortamında anonimliğini yitirir, izleme teknolojilerine ihtiyaç duyulmadan tanınabilir, VPN tüneli, Proxy (vekil) sunucusu ya da TOR ağı kullanması bir fayda sağlamaz.

Tuş vuruşu araştırmalarına farklı bir yaklaşım ise piyano ve klarnet sanatçıları incelenerek yapılmıştır. Müzisyenlerin parmak hareketleri kaydedilerek, tuşlara vurulma hızı, işlevsel veri analizi yöntemleri kullanılarak analiz edilmiş, müzisyenlerin hareket hızı ve ivmeleri çoklu müzikal bağlamda tutarlı bulunmuştur. Müzisyenleri tuş vuruşu analizi ve sinir ağları yardımı ile sınıflandırmak olanaklıdır [19].

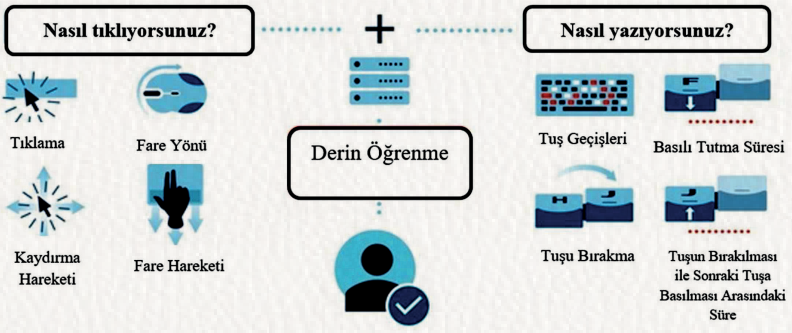
Kullanıcılar tuş vuruşlarının kaydedilmesini engellemek için bilgisayar korsanlarının yöntemlerine karşı bilinçli olmalıdır. Tuş vuruşu kayıtları ile kullanıcıların kredi kartı bilgileri, banka hesap numaraları, kullanıcı adları ve şifreleri çalınabilir, kişisel dosyaları ve e-postaları casusluk amaçlı okunup servis edilebilir. Keylogger da denilen bu izleme sistemi donanım ya da yazılım olarak kullanıcıların bilgisayarlarına yerleştirilebilir. Bilgisayarın arkasına yerleştirilen küçük bir sürücü (USB bellek gibi) ya da kullanıcının klavyeden girdiği tüm verileri kaydedip gizlice karşı tarafa gönderen bir bilgisayar programı şeklinde kullanıcılar izlenmektedir.

5.3.2. Fare Dinamiği

Fare hareketleri incelenerek de kullanıcı kimlik doğrulaması için bir davranış profili çıkartılabilir. Farenin ***x ve y*** koordinatları, yatay ve dikey hızı, teğet hız, açısal hız, teğetsel ivme, teğetsel sarsıntı, kat edilen mesafe, ortalama hız, sürükle ve bırak hareketi, tıklama verileri (tek ve çift tıklama) incelenerek bir davranış modeli oluşturulur.

Fare dinamiklerine dayalı davranış profillemenin araştırıldığı bir çalışmada, deneklerin fare verileri incelenerek bir makine öğrenmesi yöntemiyle bir davranış modeli oluşturulmuş fakat denek sayısı arttıkça yöntemin başarı oranının düştüğü keşfedilmiştir. Başarıyı yükseltmek için fare verileri her bir kullanıcı için ayrı toplanmıştır. Kimlik doğrulama sırasında eğitim aşamasında elde edilen fare verileri kullanıcının güncel davranışı ile kıyaslanarak anormal davranış olup olmadığı gözlenmiştir [20].

Şekil 5.5'te klavye ve fare biyometrilerine dayalı profiller çıkarılırken hangi verilerin toplandığı gösterilmiştir.



Şekil 5.5. Donanım gerektirmeden toplanan klavye ve fare biyometrileri [21]

5.3.3. Komut Satırı Girdileri

Kullanıcının işletim sistemi ile etkileşiminde kullandığı komutların profillenmesine dayanan bir davranış biyometrisi çeşididir. Komut satırına dayalı bir sistem olması sebebiyle genel olarak UNIX işletim sistemi üzerinde araştırmalar yapılmıştır. Kullanıcıların komut bilgisi düzeylerinin birbirinden farklı olması ve belirli görevler için alıştıkları komutları seçmede tutarlı olmaları bu biyometriyi güvenilir kılmaktadır. Veri toplama süreci genellikle zaman alıcıdır, çünkü sistemin yüksek derecede doğruluk elde edebilmesi için 15.000'e kadar ayrı komutun toplanması gerekir [22].

Kullanıcıyı uzun ve kısa vadeli olarak profillemeyi amaçlayan bir çalışma, yeterince gözlem yapıldığında ve veri toplandığında UNIX komut kümesinin, yüksek doğruluk derecesine sahip bir kullanıcıyı profillemek için kullanılabileceğini göstermiştir [23]. Modellemede kullanıcının ana bilgisayarı, UNIX komut kümesi, oturum açma zamanı gibi verilerden faydalanılmıştır.

Komut satırı girdilerine dayalı sistemlerin güvenilirliğinin araştırıldığı 2008'de yapılan bir çalışmada, 9 öğrencinin UNIX komuta geçmişlerinden alınan verilerle veri setleri oluşturuldu. Oldukça zaman alan bu veri toplama sürecinde oturum açma, değişkenler, yorum satırı, döngüler gibi pek çok özelliğe dikkat edildi. Toplanan 15.000 civarında komuta dayanarak oluşturulan kullanıcı profillerinde, sistemin ortalama algılama oranı %73.13 olarak ölçüldü [24].

Komut satırı girdilerine dayalı davranış profillemesinin faydası sadece kimlik tanımlama ile sınırlı değildir. En yıkıcı siber saldırılardan biri olan maskeli saldırıya karşı tespit sistemlerinde bu biyometriden faydalanılabilir. Maskeli saldırı (Masquerade Attack) ; meşru bir kullanıcının kimlik bilgilerini ele geçiren saldırganın, elde etmiş olduğu kimlikle bilgi sızdırması ya da sistemi sabote etmeye çalışmasıyla gerçekleşir. Bu saldırının önüne geçmek için normal kullanıcı davranışında anomali tespiti yapılabilir [25].

Anomali tespiti, bireylerin veya sistemlerin davranışlarını karakterize etmeyi ve norm dışındaki davranışı tanımayı içerir. Yapılan çalışmalarda, meşru kullanıcıların belirli bir dönemde kullandıkları komutlar yüzdesine göre kategorilere ayrılarak yeni bir yöntem geliştirilmiştir [25, 26].

Saldırı tespit sistemleri ile araştırmalar esas olarak UNIX işletim sistemi dağıtımları ile çalışmıştır fakat 2006'da yapılan bir çalışma, bugün dünyada en

çok kullanılan işletim sistemi olan Windows işletim sistemi ile de profilleme yapılabileceğini göstermiştir [27]. Kullanıcılara davranış modelleri oluşturularak kullanıcıların "normal" davranışlarını profilleyen bu çalışma, daha sonra bu modellerin oturum açma kimliğini doğrulamak veya kötü niyetli bir kişiyi tanımlamak amacı taşımaktadır.

5.3.4. Grafiksel Kullanıcı Arayüzü (Graphical User Interface - GUI)

Grafik ara yüzü sistemlerinin gelişmesiyle komut satırı verilerine dayalı kimlik doğrulama sistemlerinin yerini grafik kullanıcı ara yüzüne dayalı sistemler almaya başladı. Grafik ara yüzü sistemleri komut satırıyla kullanılabilen sistemlere göre daha çok kişiye ulaşıyordu ve daha kapsamlı veriler içeriyordu.

Başlat menüsüne tıklama, oturum açma/kapama, web tarayıcı kullanımı, .exe dosyaları tercihleri gibi veriler ile kullanıcının "ne" yaptığından çok "nasıl" yaptığı araştırıldı. Grafik ara yüzü verilerine dayanılarak yapılan kimlik doğrulamalarında %96.15 oranında başarı sağlandı. Yanlış pozitif oranı %3.85 idi [28].

5.4. MOTOR BECERİYE DAYALI DAVRANIŞSAL BİYOMETRİ

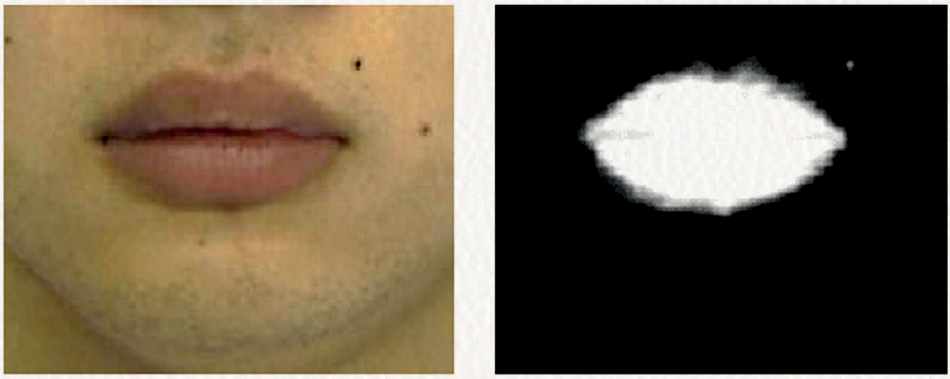
Motor beceri; bir insanın kaslarını kullanma yeteneğidir ve kalıtsal değildir. Kullanıcının bir görevi yerine getirirken doğuştan gelen kas hareketlerine dayanan biyometri sistemidir. Kimlik doğrulaması sinir, hareket, kas sistemi ve eklemlerin düzgün ve uyumlu çalışması esasına dayanır.

Motor beceriye dayalı davranışsal biyometri çeşitleri:

- Dudak hareketleri,
- Göz kırpma,
- Yürüyüş,
- Dinamik yüz özellikleri,
- Dokunsal biyometri/haptik,
- İmza/el yazısı,
- Ses.

5.4.1. Dudak Hareketleri

Dudak dinamikleri konuşmacı tanımlamadan kimlik doğrulamaya pek çok araştırmanın konusu olmuştur. Dudak okumaya dayalı konuşmacı tanımlama deneyi, görsel özellikler konuşan yüzün görüntü dizilerinden çıkarılarak yapılmıştır [29]. Şekil 5.6'da iç dudak noktaları biyoloji çeşidine ait örnek verilmiştir.



Şekil 5.6. İç dudak noktaları [29]

Ağız genişliği, üst ve alt dudak genişliği, dudak açıklığı ve yüksekliği, yatay dudak çizgisi ile üst dudak arasındaki mesafe gibi özellikler incelenerek dudak dinamiği profili oluşturulur.

Kimlik doğrulaması için yapılan bir çalışmada ise, konuşma sırasında çekilmiş videodan dudak bölgesi çıkarılmış ve konturlarının önemli özellikleri incelenmiştir. Çalışmada, ifade özelliklerini yansıtan özellik parametrelerinin diferansiyel değişimi de dikkate alınmıştır [30].

Tipik olarak dudak dinamiği, genellikle konuşmacı tanıma tabanlı kimlik doğrulaması ile birleştirilen çok modlu bir biyometrik sistemin bir parçası olarak kullanılır [31].

Dudak okuma biyometrileri ses tabanlı biyometrik sistemlerden farklı olarak konuşma engelli kullanıcılar tarafından da kullanılabileceğinden ATM'lerde finansal işlemlerde (elektronik ödeme, kimlik doğrulama vb.) ve yüksek güvenlikli merkezlere erişimde kullanılması uygun olacaktır.

5.4.2. Göz Kırpma

Bu biyometri alınırken, kullanıcı sistem kamerasına bakarak önceden belirlenmiş olan bir "göz kırpma kalıbı" (pattern) üretir.

Yapılan göz kırpma dinamiklerine dayalı bir çalışmada, kalıp bir ritme (seçilen popüler bir şarkının ritmine) uygun olarak alınıp, kimlik doğrulama aşamasında kullanıcının göz kırpma kalıbı veri tabanındaki kalıplarla karşılaştırılmıştır. Kalıp çıkarılırken göz açma ve kapama arasındaki süre ve her göz kırpmada gözün ne kadar süreyle kapalı tutulduğu gibi özelliklerden yardım alınır [32].

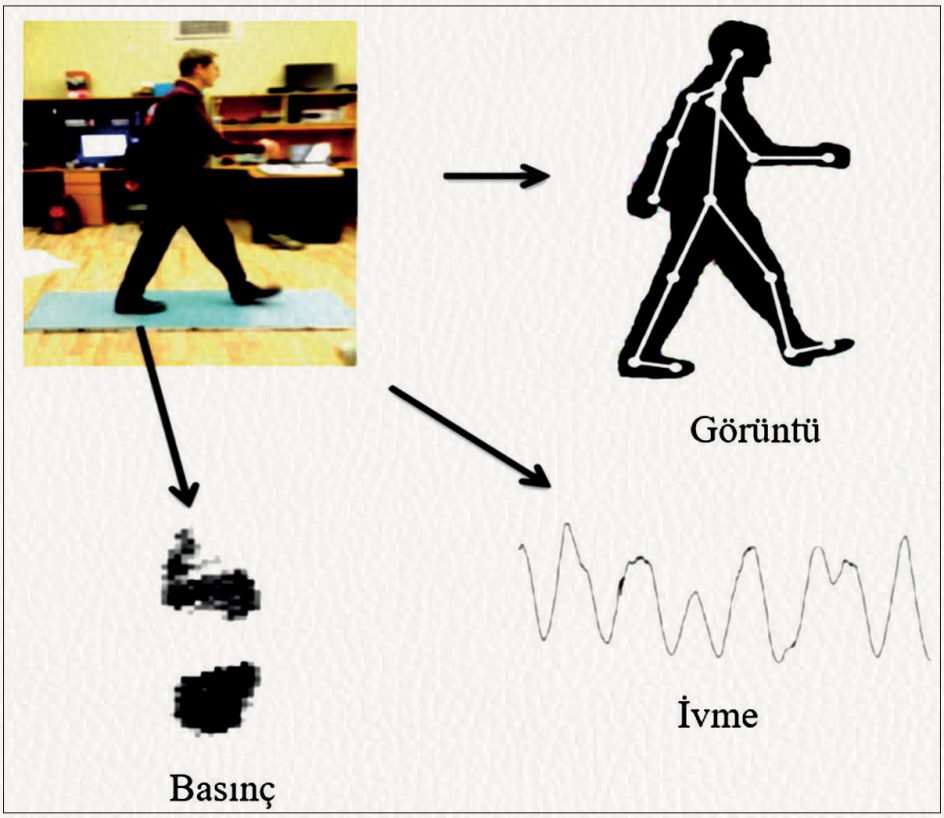
Bir başka çalışmada ise göz izleyicileri kullanılarak kullanıcıların parolalarını bakışları ile girmeleri sağlanmaya çalışılmıştır. Çalışmada kullanıcıların parolalarını girmek için ekran klavyesindeki simgelere bakarak kimliklerini doğrulamaları hedeflenmiştir. Bakış noktaları kullanıcının seçtiği sembolleri belirlemek için otomatik olarak kümelenerek kullanıcıların doğal hızlarında kimlik doğrulaması yapmaları sağlanmıştır [33].

Göz hareketleri ve bakış tabanlı biyometriler ATM işlemleri ya da alışveriş sıraları gibi halka açık/genel ortamlarda kullanıcının etkileşiminin kayıt altına alınması gibi tehditlere karşı kullanılması uygun yeni nesil bir güvenlik önlemidir.

5.4.3. Yürüyüş

İnsanların ve hayvanların yürüme biçimlerinin bilimsel analizi Antik Yunanistan ve Aristo'ya kadar uzanır. Her insanın yürüyüşü benzersiz olduğundan bu biyometri insanları yürüyüş biçimlerinden tanımlayabilmek amacıyla kullanılır.

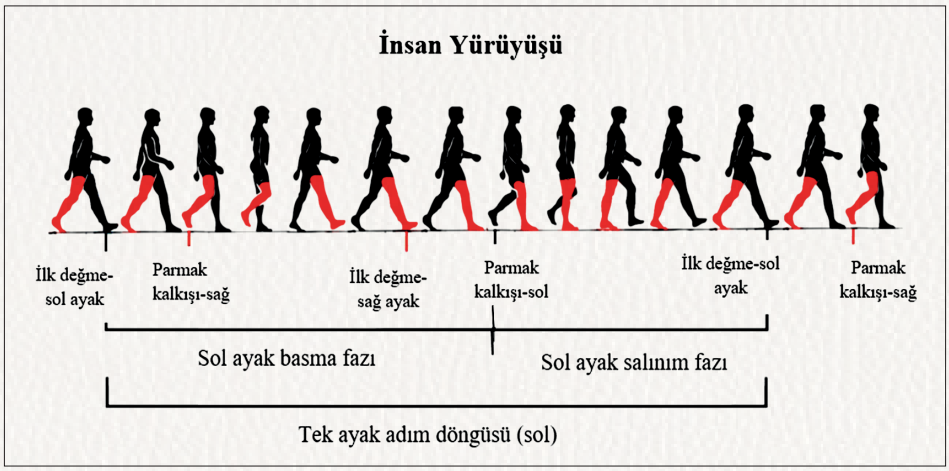
Yürüyüş stili kişinin vücut ağırlığındaki değişikliklere, taşıdığı yüklere, giyilen kıyafet ve ayakkabı seçimine, zemin yüzeyine, hamilelik sırasındaki yürüyüş güçlüğüne ve sinir sistemi rahatsızlıklarına bağlı olarak değişiklik gösterebilir [34, 35]. Yürüyüş profili çıkarılırken çeşitli yaklaşımlar kullanılabilir. Şekil 5.7'de üç farklı yöntem gösterilmiştir.



Şekil 5.7. Yürüyüş biyometrisi tanımlama için kullanılan teknolojiler [36]

a) Görüntü (Vision): Bir dizi görüntü ya da videodan yürüyüş özellikleri çıkarılır. Genellikle bir siluet ya da iskelet yapısına dönüştürülür.
b) Basınç (Pressure): Basınç sensörlü mat yardımıyla ayakaltı basıncı ölçümü ile yürüyüş özellikleri tespit edilir.
c) İvme (Accelerometry): Bir ivmeölçer ya da giyilebilir cihaz yardımıyla ivme izi kaydedilerek yürüyüş özellikleri çıkarılır.
d) Ses kaydı yapılır [36].

Yürüyüş profili çıkarılırken; kol salınımı, yürüme ritmi, adım uzunluğu, baş ve ayak arasındaki dikey mesafe, baş ve pelvis arasındaki mesafe, sol ve sağ ayak arasındaki maksimum mesafe gibi özellikler dikkate alınır. Şekil 5.8'de insan yürüyüşü aşamaları gösterilmiştir.



Şekil 5.8. İnsan yürüyüşü aşamaları [37]

Yürüyüş bir ayağın yer ile teması ile aynı ayağın ikinci kez yerle teması arasında gerçekleşir. Modern yürüme analizi, laboratuvarlarda hastanın yürüyüşü önce göz ile sonra video kayıtları izlenerek yapılır. Hastanın gövdesinde uygun noktalara bağlanan vericilerle hareket verileri bilgisayara aktarılır. Sonrasında yere monte edilmiş bir kuvvet platformuna basarken ölçülen yer tepkimesi kuvveti değişimleri de bilgisayara yüklenir [38]. Oldukça güvenilir bir biyometri çeşidi olan yürüyüş, 2000 yılında Londra'da bir hırsızlık davasında adli kanıt olarak da sunulmuştur. (Suç mahalleri, İngiltere ve diğer yerlerdeki bilinen şüphelilerin yürüyüş videoları ile karşılaştırıldı.)

Yürüyüş biyometrisine popüler bir örnek vermek gerekirse, Görevimiz Tehlike film serisinin 2015 yapımı 5. filminde *(Mission: Impossible - Rogue Nation)* yürüyüş biyometrisinin güvenliğinin altı çizilmiştir. Güvenlik protokolünün bir parçası olarak yürüyüş analizi kullanan bir binaya sızmak zorunda kalan IMF ajanı Benji Dunn (Simon Pegg) bunu yazılımı hackleyerek yapabilmiştir.

5.4.4. Dinamik Yüz Özellikleri

Statik yüz tanımasından farklı bir biyometri çeşididir. Yüz ifadesi sırasında cilt gözeneklerinin hareketini izler [39]. Bunun için bir nötr ifadeli ve bir yüz ifadesine sahip iki görüntü alınır. (İfade gülümseme olabilir.) Yüz derisinin altındaki kasların karakteristik deseni analiz edilir. Kişi gülümserken ağız etrafındaki derinin hareketi incelenerek gülümseme profili çıkarılır. Yüz hare-

ketleri, bireye özgü karmaşık bir dizi kas hareketinden oluştuğu için, bir bireyin yüz ifadelerini taklit etmek neredeyse imkânsızdır. Bu hareketler kaslar tarafından kontrol edildiğinden gülümsemenin derecesinden ya da makyajdan etkilenmez [40].

Dinamik yüz özellikleri 4 megapikselden yüksek çözünürlüklü bir dijital kamera ile çıkarılabilmiştir, günümüz ortalama 20 megapikselli akıllı telefonları düşünüldüğünde yüksek güvenlik gerektiren merkezlerde yüz hareketleri biyometrileri rahatlıkla kullanılabilir. Yüz tanıma sistemlerinin fotoğraflarla aldatılabildiği günümüzde hafifçe gülümseme gibi yüz hareketleri ile doğrulamanın önemi artacaktır.

5.4.5. Dokunsal Biyometri / Haptik (Mobil Etkileşimler)

Haptik teknolojisi, kullanıcıların dokunarak bilgisayar tabanlı bir uygulama ile etkileşime geçmelerini sağlayan teknolojidir. Yunanca Haptikos (dokunma ile ilgili) sözcüğünden türeyen bu teknoloji 1970'lerde geliştirilmeye başlanmış ve günümüzde oyunlarda, tıp ve diş hekimliği cerrahisi öğrencilerinin eğitiminde, akıllı cep telefonları ve tablet bilgisayarlarda kullanılmaktadır. Haptik teknoloji kavranabilir (haptik cihazlar), giyilebilir (kablolu eldivenler) ya da dokunmatik (ekranlar) şekilde kullanılabilir.

Dokunsal sistemler, kullanıcının etkileşimlerinin yönü, basıncı, kuvveti, açısı, hızı ve konumu hakkında bilgi sağlayabilen bilgisayar giriş/çıkış cihazlarıdır. Dokunsal bir kalemden (haptic pen) veri toplanırken tuş vuruşu süresi, kalemin konumu, telefon ekranına uygulanan kuvvet, tıklama ve çift tıklama, kaydırma hareketi, başparmak uzunluğu ve basılı tutma süresi gibi özellikler dikkate alınarak yapılan bir çalışmada, kullanıcıların yaklaşık %80'inin standart sapmanın 3 kat eşiği ile doğrulama olasılığı ile kabul edilebilir bir performans gösterdiği görülmüştür. Deneysel sonuçlar en iyi performansın kalemin pozisyonu ile ilgili veriler sayesinde olduğunu ortaya koymaktadır. Bu özellikler bireyleri tanımak için ağırlıklı değer sağlamıştır [41].

Dokunsal biyometrinin daha etkili olabilmesi için kavrayış biyometrisi, bireyin bir mobil cihazı tutma veya işleme şekli ile beraber kullanımı önerilebilir. Kullanıcıların dokunmatik cihazlarını ayakta dururken, düz otururken, geriye doğru otururken, öne doğru eğilmiş olarak otururken, kollar bir masa üzerinde olacak şekilde otururken ve bir koltukta uzanırken nasıl kullandıklarının incelendiği bir çalışmada akıllı telefonlarda duruş tanıma metotları önerilmiştir [42].

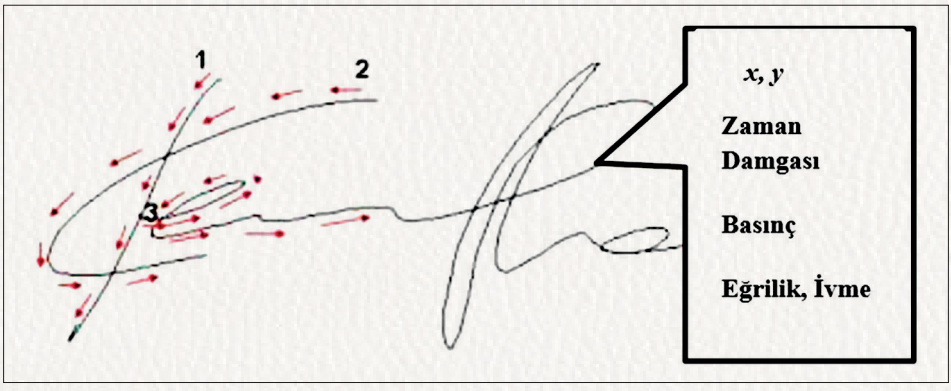
5.4.6. İmza / El Yazısı

İmza, kimlik doğrulaması için yaygın olarak kullanılan bir yöntemdir. Formlar, sözleşmeler, senetler gibi pek çok belge için vazgeçilmez olduğundan imzaların pratik şekilde ve hızlı doğrulanması oldukça önemlidir. İmza doğrulama çevrimiçi doğrulama ve çevrimdışı doğrulama olmak üzere iki grupta incelenir.

Çevrimiçi imza doğrulaması, imza doğrulama sistemini kullanarak yazarın kimliğini doğrulama işlemidir. Çevrimiçi doğrulama için sayısallaştırma tableti ve USB bağlantı noktasına bağlı, basınca duyarlı özel bir kalem gerekir. İmza, x-y koordinatlarından oluşan kalem darbeleri olarak karakterize edilir ve veriler imza veri tabanında bir txt.file biçiminde depolanır [43]. Yapılan çalışmada veri tabanında saklanan imzalar ile kullanıcının mevcut imzası karşılaştırılarak sahteciliğin önüne geçmek hedeflenmiştir.

Çevrimdışı imza doğrulama sistemleri bir imzanın taranmış görüntüsünde çalışır [44]. İmzanın görüntüsü, imzalama gerçekleştikten bir süre sonra bir tarama cihazı kullanılarak elde edilir. Çevrimiçi imza doğrulama yöntemi çevrimdışı modda bulunmayan özellikler elde ettiğinden, dinamik imza doğrulaması daha güvenilirdir [45].

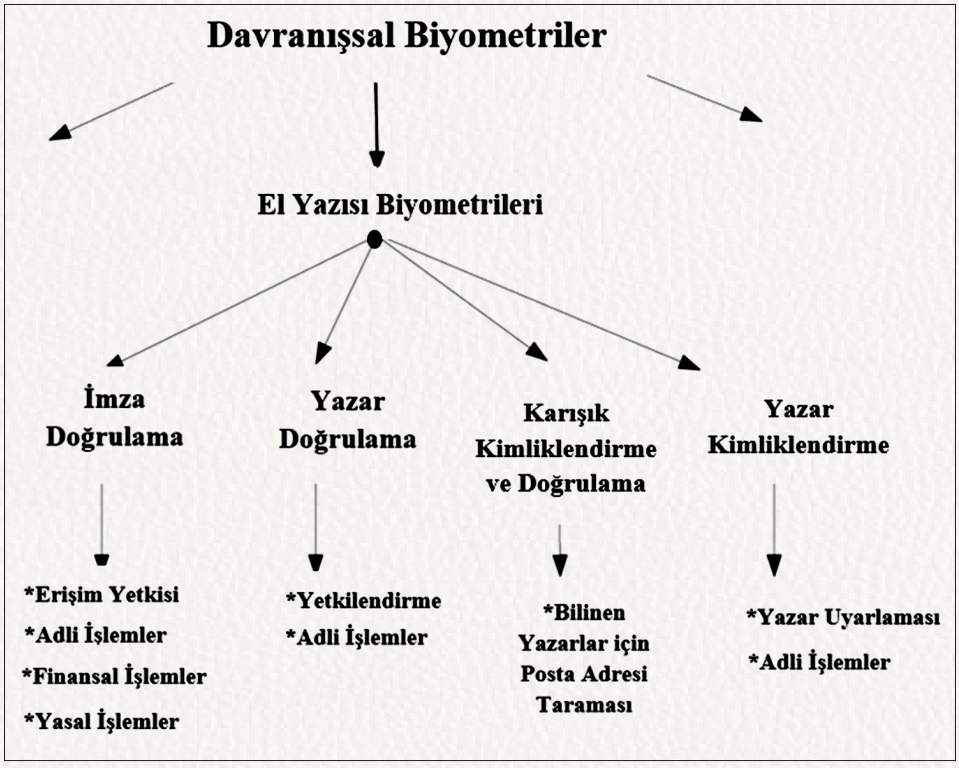
İmza profili çıkarılırken imzanın x-y koordinatları ve yörüngesi, imza akışı, kontur, kalem ucu basıncı, ivme ve kalem eğimi, imzalama hızı ve imza sınırlama kutusu gibi özelliklerden faydalanılır. Kopya makinesi ya da deneyimli bir dolandırıcı imzaları duplike edebilir ancak çevrimiçi doğrulamada imza atan kişinin oluşturduğu imza deseni, ivmesi ve basıncı gibi özellikler de doğrulanmış olur [46]. Şekil 5.9'da çevrimiçi imzadan alınan özellikler gösterilmiştir.



Şekil 5.9. Çevrimiçi imzadan alınan özellikler [46]

İmza tabanlı kullanıcı doğrulaması aslında bir el yazısı tabanlı biyometrik kimlik doğrulama türüdür [47]. Fakat el yazısında tanıma ve doğrulama içerikten bağımsız gerçekleşir. Süreç bu sebeple olduğundan daha karmaşık hâle gelmektedir. El yazısı biyometrisi ile imza doğrulama ve kullanıcı kimliklendirme yapılabilir.

İmza doğrulaması genel olarak yazarın aynı metni (örneğin adını) yazmasını gerektirdiği için içeriğe bağlı tanımlama yöntemleri ile yapılmaktadır. İçerikten bağımsız imza doğrulaması yapmayı hedefleyen bir araştırma el yazısını bazı özel doku içeren bir görüntü olarak alarak yazarını doku tanımlaması şeklinde belirleyebilmiştir. Yöntem Çince el yazısı ile 17 kişi üzerinde denenmiş ve umut veren sonuçlar alınmıştır [48]. Şekil 5.10'da el yazısı biyometrisi ve kullanım alanları gösterilmiştir.



Şekil 5.10. El yazısı biyometrisi ve kullanım alanları [49]

El yazısı ve imza tabanlı kullanıcı doğrulamaları, kimlik bilgilerinin güvenli ve hızlıca onaylanmasının gerektiği bankacılık ve finans, hukuki işlemler ve adli vakalar için oldukça önemli bir teknolojidir [49].

5.4.7. Ses

Ses tanımlama en iyi araştırılan biyometrik teknolojilerden biridir. Ses tanımlama sistemi söylenenlerin özgünlüğüne göre üç grupta incelenir:

- Sabit Metne Dayalı Sistemler: Konuşmacı kayıt sırasında seçilen belirli kelimeyi söyler.
- Metne Bağlı Sistemler: Konuşmacıdan sistem tarafından belirli bir cümle söylemesi istenir.
- Metinden Bağımsız Sistemler: Konuşmacı istediği kelimeleri söylemekte özgürdür [50].

Profil oluşturulurken konuşmacının vokal yolu, anatomik yapısı, ses perdesi, ses frekansı, gırtlağın tonu, ses tonu ve armonisi gibi veriler dikkate alınır. Ses tanımlama sistemleri iki farklı şekilde kullanılabilir; belirli bir konuşmacının kimliğini tanımlamak veya konuşmacının iddia ettiği kimliği doğrulamak [51].

Mevcut konuşmacının sesinin belirli özelliklerinin, önceden kaydedilmiş konuşmacıların özelliklerini (vektörlerini) içeren bilgisayar tabanı ile karşılaştırılmasıyla yapılan bir deneyde, konuşmacı doğrulaması için yeni bir yöntem dile getirilmiştir [52].

Ses tanımlama için yapılan modeller düşük ve yüksek seviye olarak gruplanabilir. Düşük seviye modellerde periyot, ritim, ton, frekans, spektral büyüklük ve bant genişliği gibi özelliklerden yararlanılırken yüksek seviyeli modeller için; diyalekt (lehçe), aksan ve konuşma stili gibi daha gelişmiş özellikler de dikkate alınır [53]. Standart Amerikan İngilizcesi ve Hint Aksanlı İngilizce arasında ayrım yapmayı hedefleyen bir çalışma konuşmacı tanımlamada aksanın önemini ortaya koymuştur. Konuşmacı kimliği ve içerikten bağımsız olarak "konuşma" aksan ve cinsiyet gibi yumuşak davranışsal biyometriler (*) hakkında bilgi vermiştir. Cinsiyet ve vurgu verileri konuşmacı tanımlama sistemlerinin performansını arttıracaktır [54]. Bu amaçla aksana özgü kelime modelleri kullanılabilir.

Aksanlar üzerine yapılan bir başka çalışma ise aksan sınıflandırmasının mümkün olabildiğini göstermiştir. Cinsiyet sınıflandırma temeline inşa edilen bu

çalışmada Amerikan aksanını ve İngiliz aksanını ayırt etme doğruluğu %83 olarak tespit edilmiştir [55].

Konuşma tanıma sistemi aksan ve vurgular gibi özelliklerin yanı sıra kahkaha sesini de ayırt edebilmelidir. Bir diyalogda gözlemlenen en yaygın mimik gülümsemedir, bu sebeple kahkaha sistem tarafından anlamlı kelimeler olarak algılanabilir. Kahkaha seslerini tespit etmeye çalışan bir araştırma doğal konuşma videolarından %70 oranında kahkaha ses algılama verisi elde etmiştir [56].

Konuşmacı tanımlama ya da kimlik doğrulama çalışma alanı sadece "konuşma" ile sınırlı değildir. Ses biyometrisi araştırmacıları bir şarkıyı kimin söylediği sorusuna da cevap aramıştır. Yapılan bir çalışmada şarkıcının kimliği, bir müzik kaydında belirli bir şarkıcının olup olmadığı veya ne zaman mevcut olduğu tespit edilmeye çalışılmıştır.

Ses modellemesi yapılırken şarkıcı sesinin karakteristik özelliklerinin ses tonlama tespiti ile müzikten çıkarılmış ardından vokal sinyalin istatistiksel analizini yapılarak solo ses modeli elde edilmiştir. Bu özelliklerin yanı sıra çeşitli müzik stilleri, müzik türleri ve dil gibi müzik verilerine ihtiyaç duyulmuştur. Solo ve düet parçalarından oluşan bir pop müzik veri tabanı üzerinde yapılan deneysel değerlendirmeler, önerilen yöntemlerin geçerliliğini doğrulamıştır [57].

Ses tabanlı biyometri sistemlerinin doğruluğu dudak dinamikleri de eklenerek arttırılabilir. Soğuk algınlığı, aksan farklılığı, duygulara göre değişen vurgular ses tanıma sistemleri üzerinde dezavantaj yaratabilir.

Ses tanıma ve dudak okuma analizlerine gerçekçi bir örnek Stanley Kubrick'in 1968 yapımı 2001: Uzay Yolu Macerası *(2001: A Space Odyssey)* filminde verilmiştir. Uzay gemisinin bilgisayarı HAL 9000, konuşmaları anlayabilmekte, yüzleri tanıyabilmekte, bir insan gibi konuşabilmekte, dudak okuyabilmekte ve mimikleri değerlendirebilmektedir. HAL 9000, bugün Amazon Echo gibi sesle etkinleştirilen ev yardımcılarını hatırlatmaktadır.

- ***Yumuşak Davranışsal Biyometri*:** Cinsiyet, etnik köken, yaş, boy, kilo ve göz rengi gibi özellikler benzersiz ve güvenilir olmasa da, kullanıcı hakkında bazı bilgiler sağlar. Bu özellikler yumuşak davranışsal biyometri adını alır ve birincil biyometrik tanımlayıcılar tarafından sağlanan kimlik bilgilerini tamamlar. IQ testi sonuçları, yabancı diller üzerindeki yetkinlik, araba ya da uçak kullanabilme gibi yetenekler de bu biyometri kapsamındadır [58].

5.5. SAF DAVRANIŞSAL BİYOMETRİ

Saf davranışsal biyometriler; insan vücudunun ölçümlerine değil, tamamen davranışa odaklı bir biyometri sistemidir. Taklit edilemeyen insan davranışını, kısaca insanı ölçer. Bu davranışlar arasında kullanıcının stratejileri, bilgi birikimi, yetenekleri ve tecrübeleri yer alır.

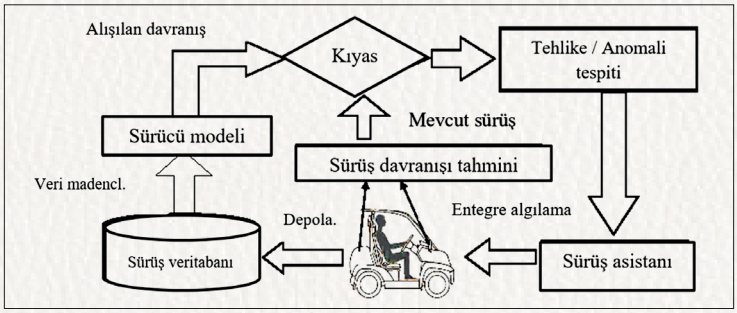
Saf davranışsal biyometri çeşitleri:

- Araba sürüş stili,
- Oyun stratejileri,
- Kredi kartı kullanımı,
- Çağrı alışkanlıkları,
- Programlama stilleri.

5.5.1. Araba Sürüş Stili

İnsanların araç kullanma eğilimleri birbirlerinden oldukça farklıdır. Sürücünün güvenli yol tutuşu, hız limitlerine uyması ya da sürüşte agresif bir tutum sergilemesi gibi alışkanlıkları farklı sürüş stilleri meydana getirmektedir. Yapılan profilleme çalışmasında sürücü davranışı modellenirken gaz ve fren pedalının basınç değerleri, dakikadaki devir cinsinden aracın hızı, trafik ve bu aralıktaki direksiyon açısı verileri toplanmıştır [59].

Bir başka çalışmada ise önceden onaylanmış bir sürücü davranış modeli kullanılarak olası sürücü niyetini tahmin etmek amaçlanmıştır. Her modelin simüle edilmiş davranışını sürücünün gerçek gözlemlenen davranışıyla karşılaştırarak şerit değişiklikleri tespit edilmeye çalışılmıştır [60]. Şekil 5.11'de araba sürücü stili biyometrisine ait örnek verilmiştir.



Şekil 5.11. Sürücü profilleme sistemi [61]

Sürüş stilinin profillenmesi; aracın kişiselleştirilmesi ile hırsızlık önleme, sürüşte anomali saptanması ile yorgun ya da sarhoş sürücü tespiti gibi avantajlar sağlar. Öte yandan sigorta şirketlerinin bu hassas verileri ele geçirmesi sürücülerin sürüş tarzlarını inceleyerek sigorta kapsamlarını genişletmemesi gibi dezavantajlar doğurabilir.

5.5.2. Oyun Stratejileri

Oyuncu stratejisi profili oyunun tüm aşamalarında oyuncunun dikkate aldığı kart aralığını gösteren frekans ölçülerinden oluşur. Oyuncuların tarzlarına göre ne zaman flop oynayacakları, açılış hareketlerinin türü ve bu hareketleri ne kadar erken yaptıkları gibi gözlenebilir veriler incelenerek bir davranış modeli oluşturulabilir. Poker oyununu baz alan bir araştırmada oluşturulan davranış modeli ile oyuncunun oyun sırasındaki hamleleri sürekli karşılaştırılarak davranışta önemli bir sapma olup olmadığı gözlenmiştir. Önemli sapmalar potansiyel güvenlik ihlali olarak oyun sunucusu yöneticisine bildirilerek kullanıcı doğrulaması yapılabileceği sonucuna ulaşılmıştır [62].

Bilgisayar ile oynanan satranç oyunlarında yapılan analizlerde ise oyuncuların gelecekteki hareketlerini tahmin etme yaklaşımı ile rakip doğrulama yapılan bir çalışma mevcuttur [63]. Yapılan bu profilleme oyuncunun rakipleri tarafından elde edildiğinde, oyuncunun oyunundaki zayıflıkları bulmak ve haksız avantaj sağlamak için analiz edilebilir. Davranış tahmin modeli çıkarılan bir rakibe karşı üstünlük sağlanabilir, bu da adil bir oyun sunmaz.

5.5.3. Kredi Kartı Kullanımı

Yaşanan teknoloji çağı geçmişten gelen, para harcama da dâhil, birçok alışkanlığı değiştirmiştir. Günümüzde insanlar yanlarında nakit para taşımak, ATM aramak ya da hızlı ve kolay şekilde ödeme yapabilmek için kredi kartı kullanma alışkanlığı kazanmıştır. Kredi kartları ile internet ortamında online alışveriş yapılabilmesi imkânı kredi kartı kullanımını siber suçların konusu hâline getirmiştir.

Hesap numarası, işlem türü, kredi kartı türü, kart kimliğinin kimliği ve adresi gibi verilerle davranış profili oluşturulur. Kartla yapılan alışılmadık işlemler, uzak coğrafi bölgelere yapılan ödemeler, kartın eş zamanlı birkaç yerde kullanılması gibi verilerin tespiti ile kart hırsızlıklarının önüne geçi-

lebilmektedir [64]. Kredi kartı kullanımına dayalı davranışsal biyometriler veri madenciliği tekniklerinin yardımıyla kredi kartı sahtekarlıklarının tespitinde kullanılmaktadır.

Kredi kartı kullanımı verileri ile meydana gelebilecek sahtekarlıklar bankalara müşteri davranışlarını profilleme sorumluluğu yüklemektedir. Aynı üründen birden fazla yapılan sipariş, alışılmadık coğrafi bölgelere ödeme yapılması, alışılmadık fatura ve teslimat adresi, kullanılan kart sayısı, online alışverişte kullanılan alışılmadık IP adresi, sepet ortalaması üzerinde verilen siparişler, kartın kullanım sıklığının değişmesi, aynı kartın farklı üyeliklerde kullanılması, fatura ve teslimat adreslerinin birbirinden farklı olması gibi noktalar belirlenip çoğaltılarak alışverişler izlenmelidir.

5.5.4. Çağrı Alışkanlıkları

Cep telefonu şirketleri artan dolandırıcılık faaliyetleri yüzünden davranış profilleme yöntemini kullanmaya başlamıştır. Sahtekarlıkları tespit etmek için kullanıcı davranışlarının izlendiği bir çalışmada veri madenciliği tekniklerinden faydalanılarak müşteri davranışları profillenmiştir. Uzak bir coğrafi bölgeden gelen, 1 dakikadan az süren ve gece yarısı yapılan aramalar gibi olağandışı davranışlar tespit edildiğinde sistem alarm vererek müşteriyi bilgilendirmektedir [65, 66].

Görüşme tarihi ve saati, görüşmenin süresi, aranan numara, arayan numara, aramanın coğrafi kökeni, ankesörlü ya da mobil telefon kullanımı, çağrı maliyeti, yerel ve mobil hedeflere yapılan çağrı sayıları, uluslararası hedeflere yapılan çağrı sayıları gibi özellikler tespit edilerek kullanıcı için bir davranış modeli oluşturulur.

5.5.5. Programlama (Kodlama) Stilleri

Siber suçların günümüzde hızla artması kamu kurumlarını, üniversiteleri, bankaları, şirketleri ve internet kullanan herkes için bir tehdit oluşturmaktadır. Virüsler, solucanlar, Truva atları ve daha birçok kaynak kod güvenliğimiz için tehlike oluştururken anonimlik sebebiyle izleri sürülememektedir. Fakat kaynak kod analizi ile kötü amaçlı yazılımın yazarını tanımlamak adli bir araştırma için son derece faydalı olacaktır [67].

Bu tanımlama için çıkarılacak davranış modeli; seçilen programlama dili, kod biçimlendirme stili, kod düzenleyici türü, değişken adları, döngü yapılarının seçimi, yazım ve dilbilgisi gibi özellikler incelenerek oluşturulur.

Programlama davranış modellerinin araştırıldığı bir çalışmada 5 basamak ortaya konmuştur [68].

- Yazar Kimliği: Yazar kimliği tespit edilirken bir kod parçasının belirli bir yazara ait olup olmadığı araştırılır. Metin yazarlığı biyometrilerinde olduğu gibi kod parçası yazara ait olduğu bilinen program örnekleri ile karşılaştırılır.
- Yazar Karakterinin Çıkarımı: Bu uygulama alanı, programlama tarzına bağlı olarak, programcının kültürel eğitim durumu ve program diline olan aşinalığı gibi bir kod parçasının teknik özelliklerini belirler.
- İntihal Tespiti: Bu yöntem, birden çok kaynak kod dosyası kümesi arasındaki benzerlikleri bulmaya çalışır. Aynı zamanda başka birine ait çalışmanın uygun onay alınmadan kullanılması dışında eser hırsızlığını tespit edebilecek bir yöntemdir.
- Yazar Ayrımcılığı: Kod parçalarının tek bir yazar tarafından mı yoksa birkaç yazar tarafından mı yazıldığına karar verme amacı taşır. Buna bir örnek, bir programın muhtemelen söz konusu yazarları tanımlamaksızın üç farklı yazar tarafından yazıldığını gösterebilir.
- Yazarın Niyetinin Belirlenmesi: Bir zarara neden olan kod parçasının, kasti olarak yazılıp yazılmadığını anlamak gerekir. Yazılım geliştirme işlemi sırasındaki bir hata ciddi sorunlara neden olabilir.

Sınırlı sayıda katılımcı ile yukarıda saydığımız özellikler incelenerek yapılan çalışmalarda program yazarını belirlemek mümkün olmuştur.

5.6. DAVRANIŞSAL BİYOMETRİ KARŞILAŞTIRILMALARI

Davranışsal biyometrik sistemlerin güvenli kabul edilebilmesi için sağlamaları gereken 7 önemli ilke bulunmaktadır; evrensellik, teklik/tekillik, kalıcılık, toplanabilirlik, performans/verim, kabul edilebilirlik, tehdidi önleme veya tehdide dayanıklılık. Tablo 5.1'de biyometrik teknolojilerin bu ilkelere göre karşılaştırılması yapılmıştır. Tablo 5.2'de ise davranışsal biyometriler geleneksel kimlik doğrulama sistemleri ile karşılaştırılmıştır.

Tablo 5.1. Biyometrik teknolojilerin güvenlik ilkelerine göre karşılaştırılması [69]

	Evrensellik	Ayırt Edicilik	Kalıcılık	Toplanabilirlik	Kabul Edilebilirlik	Verim	Tehdide Dayanıklılık
Fare Hareketleri	Düşük	Düşük	Düşük	Orta	Orta	Düşük	Orta
Tuş Dinamikleri	Düşük	Düşük	Düşük	Orta	Orta	Düşük	Orta
Ses	Orta	Orta	Düşük	Orta	Yüksek	Orta	Düşük
Yürüyüş	Yüksek	Düşük	Düşük	Yüksek	Düşük	Orta	Düşük
İmza	Düşük	Düşük	Düşük	Orta	Yüksek	Orta	Orta

* Davranışsal biyometriler farklı insanların farklı yeteneklerine bağlı olmasına karşın spesifik bir davranış üzerinde profilleme yapılıyorsa evrensellik ilkesine %100 uymaktadır.
* Saf davranışsal biyometriler ya da kaynak tabanlı biyometriler dışında incelenen davranışsal biyometrilerin teklik ilkesine uyma yüzdeleri düşüktür.
* Davranışsal biyometri yöntemleri kullanıcının ruh hâlinin ve alışkanlıklarının zamanla değişebilmesi nedeniyle kalıcılık garanti etmez. Ayrıca zamana bağlı olarak kullanıcıların tecrübeleri artacağından bilgi ve beceri düzeyleri gelişecek ve düşük bir kalıcılık oranı gösterecektir.
* Davranışsal biyometri verilerini toplamak fiziksel biyometri verilerini toplamaya göre oldukça kolay ve düşük maliyetlidir, özel donanım gerektirmez. Kullanıcı bilgisi olmadan bile toplanabilir. Bu sebeple davranışsal biyometriye sessiz doğrulama sistemi de denilmektedir.
* Birçok davranışsal biyometrinin doğruluğu kullanıcı sayısı arttıkça düşmektedir. Fiziksel biyometri ile kıyaslandığında davranışsal biyometrinin doğruluğunun arttırılması gerektiği açıktır. Daha ayırt edici özellikler eklenerek performans yükseltilebilir.
* Davranışsal biyometri kullanıcı katılımı olmadan toplanabildiğinden, yüksek derecede kabul edilebilirlik ilkesinden yararlanırlar ancak etik veya gizlilik nedenleriyle itiraz edilebilirler.
* Başka bir insanın davranışları hakkında derinlemesine bilgi gerektirdiğinden davranış biyometrilerinin taklidi oldukça zordur bu da tehdide dayanıklılık ilkesince avantaj sağlar.

Tabloda görülebileceği gibi genel olarak davranışsal biyometrilerin ayırt ediciliği ve kalıcılık ortalaması düşüktür, kullanıcı kimliğini tanımlayacak kadar ayırt edici değildir fakat kimlik doğrulamasında oldukça başarılı sonuçlar verir. (Örneklem küçük olduğu takdirde kullanıcı tanımlaması yapılabilir.) Daha başarılı sonuçlar almak için birkaç özellik beraber kullanılabilir. Örn; dinamik yüz özelliklerine ve sese dayalı davranış modellerinin beraber kullanımı gibi. Davranışsal biyometri ekstra bir güvenlik katmanı olarak geliştirilmiştir, bu sebeple parola/şifre sistemleriyle kullanılmaları uygundur.

Tablo 5.2. Kimlik doğrulama sistemlerinin karşılaştırılması [70]

	Güvenlik Zafiyeti	Kullanım Zorluğu	Uygunluk
Parola Doğrulaması	Yüksek	Yüksek	Düşük
Çok Katmanlı Doğrulama	Orta	Yüksek	Yüksek
Davranışsal Biyometri	Çok Düşük	Yok	Yüksek

Parola koruması ve çok katmanlı kimlik doğrulamasında güvenlik insana bağlı olması sebebiyle, zafiyetleri davranışsal biyometriden daha yüksektir. Kullanıcılar zaman içinde parolalarını unutabilir, sahip oldukları token/akıllı kartları kaybedebilir, unutabilir veya çaldırabilir. Davranışsal biyometriler, taklidi, kopyalanması ve unutulması neredeyse imkânsız olduğundan yüksek güvenliklidir. Geleneksel biyometri, güvenliği yalnızca giriş noktasında ele alırken davranışsal biyometri kullanıcı çevrimiçi olduğu sürece kimlik doğrulaması sağlar.

Çok katmanlı doğrulama ve parola koruması ayrıca doğrulama yapmak için kullanıcının bilgisine ya da sahip olduğu eşyalara ihtiyaç duyar, bu da onları kullanıcıdan habersiz bile kimlik doğrulaması yapabilen davranışsal biyometrilerden daha az kullanıcı dostu yapmaktadır. Çok katmanlı doğrulama ve biyometri kullanımı günümüz koşullarında güvenlik açısından yüksek uygunluktayken parola doğrulaması oldukça düşük kalmıştır.

5.7. DAVRANIŞSAL BİYOMETRİ VE ADLİ BİLİŞİM

Günümüzde işlenen suçların %80-90'ı dijital kanıtlarla bir şekilde bağlantılıdır. Bu vakaların çoğunda bilgisayardaki kullanıcı hesapları ve kullanıcı kimlik bilgileri hayati önem taşımaktadır.

Bir örnek olarak; Amerika'da görülen bir adli bilişim davası kimlik doğrulama yöntemlerinin güvenilirliğinin sorgulanmasına neden oldu. A kullanıcısının B kullanıcı hesabına giriş yaptığı davada mahkumiyet kararı temyiz mahkemesinde tersine çevrildi, çünkü kolluk kuvvetlerinin aile üyelerinden hangisinin "suçlu" olduğunu belirlemesine olanak yoktu [71].

Davranışsal biyometriye dayalı kimliklendirme ile kullanıcı davranışı desenleri (pattern) oluşturularak kullanıcılar birbirlerinden ayırt edilebilir. Bu teknikle ek doğrulama sistemleri geliştirilebilir, adli soruşturmalara ışık tutulabilir.

Ses tanımaya dayalı biyometrik sistemler bankacılıkta kullanılabilir, dolandırıcılık yaptığı tespit edilen kişilerden alınan sesli imzalar ile bir veri tabanı oluşturularak kara liste hazırlanabilir. Birden fazla konuşmacı içeren ses kayıtlarında ise konuşmacı sayısı ve konuşmacıların kimlikleri saptanabilir böylece adli soruşturmalarda şüpheli sayısı daraltılabilir.

Bankacılıkla ilgili bir başka bilinen adli bilişim olayı ise İngiltere'de gerçekleşmiştir. İngiltere'nin ilk beş kurumsal bankasından biri artan siber saldırılardan dolayı sorun yaşıyordu. Düzenlenen bu siber saldırılar kötü amaçlı yazılım (malware) tespiti ve izleme monitörleri gibi geleneksel kontrol sistemlerini atlatabiliyordu. Şirket çevrimiçi bankacılık uygulamalarına davranışsal biyometrik sistemi ekleyerek, riskli işlemler için gerçek zamanlı işlem uyarıları kullanarak saldırıyı hızla saptırabildiler. En dikkate değer vakalardan biri, gelişmiş bir uzaktan erişim truva atı içeren 1.6 milyon £'lık dolandırıcılık hamlesiydi [72].

Biyometrilerle ilgili ses getiren en büyük olay ise bu sayılanlardan biri değildi. Ayırt ediciliği ve kalıcılığı tartışılmaz olan fizyolojik biyometrilerin ifşası geçtiğimiz yıl Suprema şirketine ait Biostar 2 güvenlik firması tarafından açıklandı [73]. ABD'deki Union ortak çalışma alanları ve Londra Metropolitan Polisi de dâhil olmak üzere tüm dünyadaki büyük şirketlere hizmet veren şirketin, kullanıcıların yüz fotoğrafları, şifrelenmemiş kullanıcı adları ve şifreler, parmak izi ve yüz tanıma verileri de dâhil olmak üzere 27.8 milyondan fazla kayıt içeren 23 gigabaytlık bir veri tabanına erişildi. Parmak izi verilerini ele geçiren bir saldırgan uygun bir mürekkeple parmak izi kopyalayarak biyometrik tarayıcıları atlatması mümkündür [74]. Paylaşılan fotoğraflarla yüz tanıma sistemleri kandırılmış [75], sentetik iris üretme araştırmaları başarılı sonuçlar vermeye başlamış [76], yüz ve kulak verileri yardımıyla 3D yazdırılmış kafalar ile yüz tarama tabanlı güvenlik sistemleri aldatılmıştır. [75].

5.8. DAVRANIŞSAL BİYOMETRİNİN HUKUKİ DAYANAĞI

Türkiye'de vatandaşlar günde ortalama 7 saat 15 dakika internette vakit geçiriyor. Bunun 2 saat 46 dakikasını ise sosyal medyada geçirdiği vakit oluşturuyor [77]. Bu etkinlikler arkamızda çevrimiçi davranışlarımıza dair izler bırakır ve bu izler çerezler yardımıyla sürülebilir. Çerezlerin izinin sürülerek kullanıcıların kimliklerinin belirlenmesine "açık izleme" denir. İnternet kullanıcıları davranış tabanlı izleme teknikleriyle de çevrimiçi davranışlarına göre tanımlanabilir. Bu tanımlama göze çarpmayan bir şekilde ve prensipte, davranışı izlenen insanların bilgisi olmadan gerçekleşir. Bu teknik örüntü tanıma yöntemlerinden yararlanır.

Çevrimiçi davranış tanımlama veya kimlik doğrulama davranış biyometrisi alanı kapsamındadır. Kullanıcı tarafından ziyaret edilen sayfalar, oturum geçmişi, incelenen içerikler, önerilen siteler, arama istekleri, kayıtlı kullanıcılar ve kullanıcı giriş bilgileri, tıklama/kaydırma gibi eylemler, reklamlar/abonelik/iletişim formları gibi ögelerle etkileşimler ve ziyaret zamanı gibi web göz atma davranış verileri analiz edilerek kişiselleştirilmiş reklamlar oluşturulmaktadır.

Davranış biçimleri kişinin kendi kimliğinin ifadesidir ve etkili bir yasal korunmayı hak eder. 25 Mayıs 2018'de Avrupa Birliği'ne üye ülkelerde yürürlüğe giren ve kişisel verileri korumayı amaçlayan Genel Veri Koruma Yönetmeliği (General Data Protection Regulation- GDPR)'ne göre hiçbir kişisel veri, veri sahibinden açık onay alınmadığı sürece işlenemez. Veri sahibi bu izni iptal hakkına sahiptir ve yönetmelik geçmişte saklanan verileri de kapsamaktadır. Bu kişisel verilere; isim, adres TC kimlik no, fiziksel biyometri verileri, IP adresi, internet çerez verileri, hassas tıbbi veriler, ırk/köken/inanç/ideolojik fikirler ya da fiziksel görünüşe dair veriler de dâhildir.

- GDPR, md 4/4; *"profil çıkarma", bir gerçek kişinin işteki performansı, ekonomik durumu, sağlığı, kişisel tercihleri, ilgi alanları, güvenilirliği, davranışları, konumu veya hareketlerine ilişkin hususların analiz edilmesi veya tahmin edilmesi başta olmak üzere söz konusu gerçek kişiye ilişkin belirli kişisel özelliklerin değerlendirilmesi için kişisel verilerin kullanımını ihtiva eden her türlü otomatik kişisel veri işleme biçimidir;*

- GDPR, md 22/1; *"Veri sahibinin kendisi ile ilgili hukuki sonuçlar doğuran veya benzer biçimde kendisini kayda değer şekilde etkileyen profil çıkarma da dâhil olmak üzere yalnızca otomatik işleme faaliyetine dayalı bir karara tabi olmama hakkı bulunur."*

Davranışsal biyometriler yardımıyla kullanıcıların profillenmesi çevrimiçi izlenmeyen etkinliklerin ve anonimliğin sonunu getirebilir. Gizliliğin korunmasında ciddi sonuçlar doğurabilecek bu tutum, GDPR maddelerini sağlamalıdır [78].

Amerika Birleşik Devletleri'nde ise kişisel verilerin veya biyometrik verilerin toplanmasını ve kullanılmasını düzenleyen bir federal yasa yoktur. Fakat 1 Ocak 2020'de yürürlüğe giren CCPA (California Tüketici Gizlilik Yasası) biyometrik veriyi; "*bireyin DNA'sı dâhil olmak üzere, bir bireyin tek başına veya birbirleriyle veya diğer tanımlayıcı verilerle kombinasyon hâlinde kullanılabilen, bireysel kimlik oluşturmak için fizyolojik, biyolojik veya davranışsal özellikleri"* olarak tanımlamıştır ve California tüketicilerine kişisel bilgilerini ve biyometrik verilerini koruma hakları vermiştir.

Kimlik doğrulaması dışında bir insanın davranışlarını analiz ederek profillemek etik bir davranış değildir, en büyük tehlike mahremiyet ihlalidir. Toplanan biyometri verilerinin güvenli bir şekilde şifrelenmesi gerekir. Ele geçirilen bir bilginin üretilmesi çok kolay olabilir. Davranışsal biyometri verileri üçüncü şahısların ilgisini çeken içeriğe sahiptir. Kişiler profilleri sebebiyle ayrımcılığa maruz kalabilir. Biyometrik verilerimizin bir kez ele geçirilmesiyle değiştiremediğimiz bu verilerimiz sebebiyle ömür boyu risk altında kalacağımız unutulmamalıdır.

5.9. SONUÇ VE DEĞERLENDİRMELER

Biyometrik sistemler ve bu sistemlerin kullanım alanları üzerine genel bir değerlendirme yapılmak istenirse:

FAR (False Acceptance Rate): Sistemin veri tabanında bulunmayan bir kişiye ait bilgiler sunulduğunda, bu veriyi veri tabanında bulunan başka bir kişiyle eşleştirilmesinden kaynaklanan yanlış tespitlerin oranıdır.

FRR (False Reject Rate): Sistemin veri tabanında var olan kişiyi bulamaması oranıdır.

EER (Equal Error Rate): FAR ve FRR'nin birbirine eşit olduğu noktadır.

FAR, FRR ve EER ne kadar küçükse sistem ideale o kadar yakındır. Bu oranlar dikkate alındığında, tuş vuruşu dinamikleri, metin yazarlığı, imza, programlama stili ve komut satırı girdileri, fare dinamikleri, ses ve grafiksel kullanıcı arayüzü (GUI) biyometrileri en güvenilir davranışsal biyometriler olarak gösterilebilir [5].

Kimlik doğrulama için davranışsal biyometriler amaca uygun olarak seçilmelidir. Veri toplama kolaylığı, güvenilirlik ve maliyet düşüklüğü göz önünde bulundurulduğunda klavye ve fare biyometrilerinin müşteri odaklı web uygulamalarında ve finans alanında özellikle mobil bankacılık işlemlerinde kullanımı oldukça güvenli olacaktır. Davranışsal biyometriler sürekli kimlik doğrulaması yaptıklarından geleneksel doğrulama sistemleri gibi sadece tek bir web sayfasını değil tüm oturumu sürekli olarak korumuş olurlar. Öte yandan çağrı merkezlerinde (bankacılık ve cep telefonu operatörleri) ses tanımaya dayalı biyometrik sistemler (sesli imza) ile yapılması önerilen kimlik doğrulamalarında hem çağrı merkezi çalışanları hem de müşterileri için zamandan ve performanstan büyük ölçüde tasarruf edilebilir.

Parmak izi kopyalanabildiği ve diğer fizyolojik biyometriler statik olmaları sebebiyle taranmaya veya fotoğraflanmaya karşı savunmasızdır. Bu biyometriler kötü amaçlı kullanım için yeniden yapılandırılabilir. Davranışsal biyometri bilgilerin doğruluğunu gerçek bilgilerle kanıtlamak yerine kullanıcıyı çevrimiçi izleyerek sahtekarlığı engeller, bu nedenle finans merkezleri, Ar-Ge binaları, askerî üsler, kolluk kuvvetleri ve kamu güvenliği ile ilgili binalar gibi yüksek güvenlik gerektiren kritik noktalarda bilgisayar ve kamera sistemi kurularak, taklidi ve kopyalanması zor bir doğrulama yöntemi olan yürüyüş analizi kullanılabilir.

Ticaret ve pazarlama alanında ise müşteri davranışı modellemeleri yapılarak sadece müşterinin ilgi alanında olan ürünler/seçenekler öne çıkarılabilir. Kişiselleştirilmiş eğitim, ticaret, finansal analiz gibi hizmet alanları geliştirilmektedir.

Davranışsal biyometriler şirketleri ve kurumları beklenmedik iç tehditlerden koruyacaktır. İçeriden yapılan bir saldırı ya da ihlal meydana geldiğinde şirket çalışanlarının kimlikleri tanımlanabilir. Alınan aksiyonların biyometrik izleri sürülerek doğrulanmış kullanıcılarla karşılaştırılması sonucu fare ve klavye kullanımındaki nüanslar sayesinde suçlular tespit edilebilir. Davranışsal bi-

yometrileri olası saldırıların yanı sıra şirketi dikkatsizliklere karşı da korur. En sorumluluk sahibi kullanıcı bile oturumunu ve çalıştığı programları bilgisayarında açık unutabilir. Davranış biyometrilerine dayanan bir doğrulama sistemi yeni veya yetkisiz bir kullanıcının erişimini hızlı bir şekilde tespit edip buna karşı önlem alabilir. Şirket veya kurumlar içinde olabilecek tehditler bunlarla sınırlı değildir. Çalışanların hesaplarını, kullanıcı adlarını veya şifrelerini işlerin hızlı yürümesi amacıyla birbirleriyle paylaşması oldukça sık karşılaşılan bir güvenlik sorunudur. Davranış biyometrisi tabanlı kimlik doğrulama sistemleri oturum açma bilgileri doğru girilse bile gerçek kullanıcıları diğerlerinden ayırabilecek güvenliğe sahiptir.

İç saldırılar, ihlaller veya dikkatsizlikler güvenliğin en zayıf halkasının insan olduğunun bir kez daha altını çizmektedir. Özellikle çalışan sayısı fazla olan kurum veya şirketlerin yetkisiz erişim sorunları için davranışsal biyometriler ilk akla gelmesi gereken çözüm yolu olmalıdır.

Davranışsal biyometriler etkin ve güvenli doğrulama gücü sayesinde kişileri ve kurumları aynı zamanda dış tehditlerden de korumaktadır. Bugün şirketleri birçok siber saldırı tehdit etmektedir. Bu saldırıların başında kimlik hırsızlığı saldırıları, oltalama, uzaktan erişim truva atı (RAT), rubber ducky ve kimlik sahtekarlığı gelmektedir. Her biri yıkıcı etkilere sahip olan bu popüler saldırılara karşı kişi ve kurumlar davranışsal biyometrik teknolojilerden yardım almalıdır.

- **Kimlik Bilgisi Doldurma Saldırıları *(Credential stuffing):*** Kullanıcı hesaplarına yetkisiz erişmek için kimlik avı sonucunda elde edilmiş milyonlarca kullanıcı adı-parola kombinasyonunun enjekte edilmesiyle yapılan bir kaba kuvvet (brute force) saldırı çeşididir. Kimlik bilgileri mevcut bir hesapla eşleşene kadar giriş denenir. Saldırının başarıya ulaşmasında birden fazla ihlal söz konusudur. Bir tarafta kullanıcıların ifşa edilmiş kişisel verileri diğer taraftaysa şifrelerini sık değiştirmeyen ve aynı şifreleri tekrar tekrar kullanan kullanıcılardan bahsetmek gerekir. Yapılan bir ankette kullanıcıların %81'i aynı kullanıcı adı-parola kombinasyonunu birden fazla sitede kullandığını, %25'i ise aynı parolayı hemen her hesabında kullandığını ifade etmiştir [79]. Bu veriler ışığında oturum bilgilerinin çalınması çok da olağandışı bir durum değildir fakat önlem alınabilir. Davranışsal biyometrik teknolojilerin kullanımı sistemlerin savunmasını arttıracaktır.

- **Oltalama Saldırıları *(Phishing):*** Kullanıcıların kredi kartı numarası, kimlik bilgileri veya telefon numaraları gibi hassas bilgilerini öğrenmek amacıyla yapılan saldırılardır. Saldırgan resmî bir kurumdan, genellikle bankalardan, geliyormuş gibi görünen e-postalarla kullanıcının sahte bir web sayfasına gitmesini sağlar. Yönlendirildiği web sayfasında kredi kartı bilgilerini ve kimlik bilgilerini dolduran kullanıcı hassas bilgilerini saldırgana vermiş olur. Oltalama saldırıları adını, kullanıcıların genellikle tatil, zam, çekiliş, ödül veya iade alacağı yönünde cezbedici yemler olarak hazırlanmasından alır. Oltaya takılmamak için kullanıcılar e-posta içeriğini dikkatle okumalı, kötü dilbilgisi, gayriresmî ifadeler, bilgi talepleri veya gerçek olamayacak kadar iyi vaatlere dikkat etmelidir. Yönlendirilmek istenen web sayfasının alan adına ve logosuna dikkat edilmeli ve gerçekliğinden şüphe edilmelidir. Şüphe uyandıran alan adlarının lokasyonu araştırılmalıdır. Davranışsal biyometri tabanlı kimlik doğrulama sistemleri kullanıcının bağlantılara tıklamasını engelleyemez fakat sonrasında kullanıcıyı koruyabilir. Güvenli bir sisteme erişmek ve bu sistemde işlem yapmak için ele geçirdiği kimliğin verilerini kullanmak isteyen bilgisayar korsanlarını algılayabilir.
- **Uzaktan Erişim Truva Atı *(Remote Access Trojan- RAT):*** Kullanıcının cihazında (bilgisayar, tablet bilgisayar, cep telefonu vb.) arka planda ve kullanıcının bilgisi dışında çalışan trojanlardır. Trojanlar bilgisayarlarda kullanıcının yaptığı her şeyi yapabilirler. Kamera ve mikofonu açarak kayıt alma, bilgisayara dosya indirme, zararlı yazılım yayma, tuşları kaydederek (keylogger) banka hesap bilgileri ve şifreleri çalma, tarayıcı geçmişinde kayıtlı adres/şifre/form verilerini ele geçirme bunlardan bazılarıdır. Erişim bir şirket veya kuruma sağlandıysa hesap dökümleri, bilgisayarda bulunan projeler ve çalışanlara ait bilgiler de dâhil olmak üzere tüm dosyalar tehlikeye girecektir. Davranışsal biyometrik teknolojilere dayanan güvenlik sistemleri kimlik doğrulmasını arka planda sürekli yaptığından sisteme giriş yapan kullanıcının doğru kişi olup olmadığını anbean takip edecektir.
- **Rubber Ducky Saldırısı *(USB Rubber Ducky- BadUSB):*** USB görünümünde olan özel bir donanımın (ducky) bilgisayar, tablet bilgisayar ve cep telefonu gibi platformlarda kullanımını sağlayarak sisteme sızılmasıdır. Ducky işletim sistemi tarafından klavye olarak

algılanır, sistemin bu şekilde güvenini kazanan ducky çok kısa bir zaman aralığında klavye enjeksiyonu ile hedeflediği zararlı kodu (payload) işletim sistemine gömer [80]. Zararlı kod yüklenmesi ardından saldırganın sistemi ele geçirerek tüm kontrolü ele alması an meselesidir. Ducky saldırısından korunmak için öncelikle kullanıcı kendisine ait USB cihazlarını kullanmalı ve bu cihazları güvenmediği platformlara takmamalıdır. Bilgisayarına bir USB taktığında zararlı yazılım taraması yapmalı ve varsa USB'yi sanal makinede çalıştırmalıdır. Bilgisayar kullanan hemen herkesin verilerini USB ile yanında taşıdığı günümüzde, ducky oldukça popüler bir sosyal mühendislik saldırısıdır. Davranış biyometrileri tabanlı kimlik doğrulama sistemleri bu hızlı saldırıya hızlı bir cevap üretebilir. Klavye ile hızlı ve otomatik şekilde yazılan kod, değişik klavye biyometrisi olarak kayıt alına alınabilir, erken alınan bu önlemlerle saldırı engellenebilir.

- **Kimlik Sahtekârlığı *(Identity Fraud):*** Kimlik sahtekârlığı, kimlik hırsızlığından sonraki adım şeklinde kısaca açıklanabilir. Çalınan kimlik bilgileri ile yasadışı faaliyetlerde bulunulması veya birinin aldatılması kimlik sahtekârlığıdır.

Kimlik sahtekârlığından korunmak için alınması gereken önlemler kimlik hırsızlığına karşı alınması gerekenlerden çok farklı değildir. Eski akıllı telefonlar ve bilgisayarlar satılırken ya da imha edilirken hassas verilerin silindiğinden emin olunmalıdır. Kullanıcılar çevrimiçi davranışlarına da dikkat etmeli, alan adlarının http/https ayrımına ve şüpheli linklere karşı (spam veya phishing gibi) tetikte olmalıdır. Crackli dosyalar indirmemeli ve indirilen materyaller online dosya tarama sitelerinde incelenmelidir. Parola güvenliğine özen göstermeli, tahmini zor ve en az 8 karakterden oluşan küçük/büyük harf, sayı ve özel karakterler içeren bir parola seçmeli ve sık sık değiştirmelidir. Farklı hesaplar için farklı parolalar kullanılmalı çok sık tekrar edilmemelidir. Parola güvenliği evde bulunan WiFi bağlantısında da sağlanmalı ve güvenli bir parola belirlenmelidir. Herkese açık kablosuz ağlar kullanılıyorsa e-posta veya banka hesapları açılmamalı, online alışveriş yapılmamalı, ağ trafiğinin izlenmesine karşı tedbirli olunmalıdır. Cep telefonun otomatik bağlanma özelliği kapatılarak istenmeyen ağlara bağlanması engellenebilir.

Kimlik bilgilerini korumaya ifşa etmemekle başlanabilir. 2019 yılı araştırma istatistiklerine göre ortalama bir sosyal medya kullanıcısı sosyal platformlarda her gün 2 saat 16 dakika geçiriyor, bu veri sosyal ağların artık günlük hayatın bir parçası olduğunu kanıtlar niteliktedir [81]. Sosyal medya paylaşımında dikkat edilmesi gereken hususlar arasında kimlik bilgileri, adres/cep telefonu numarası ve diğer önemli iletişim bilgileri, fotoğraflar, arkadaş listeleri, anlık lokasyon bilgileri, doğum günü, ilgi alanları, iş yeri ve çalışılan pozisyonla ilgili bilgiler sayılabilir. Paylaşımlar kadar dikkat edilmesi gereken bir başka nokta da kullanılan bu platformların gizlilik ayarlarıdır. Verilerin kimlerle paylaşılacağı dikkatle okunmalı ve verilen izinler gözden geçirilmelidir. Gerekli olmadıkça yeni sosyal medya hesapları açılmamalı ve ihtiyaç duyulmayanlar kapatılmalıdır. Sosyal medya profilleri kolaya kaçılarak diğer web sitelerine giriş için kullanılmamalıdır bu verilerin daha çok yayılmasına ve güvenlik risklerinin artmasına neden olur. Tık tuzaklarına (clickbait) dikkat edilmeli ve kaynağı bilinmeyen bu sitelere sosyal ağ hesaplarıyla giriş yapılmamalı, fotoğraf yüklenmemelidir. Yönetim düzeyinde ise kullanılmayan portlar kapatılmalı ve ağ trafiği izlenmelidir.

Bankalar ve sağlık kurumları gibi kimlik doğrulamanın oldukça hayati olduğu kuruluşlar kimlik hırsızlıklarına karşı tedbirli olmak zorundadır. Davranışsal biyometrik sistemlerini kullanarak son kullanıcılar için profiller oluşturabilirler. Dolandırıcıların elinde çalıntı kimlik bilgileri bulunsa bile gerçek kullanıcıların hassas verilerine erişmeleri ve hizmet almaları engellenebilir.

Güvenliğin ancak en zayıf halka kadar iyi olduğunun vurgulanmak istendiği bu çalışmada, kullanıcıları bilgilerini korumak için kat ettiği uzun yol açıklanmaya çalışılmıştır. Siber suçların hızla arttığı ve kendisini yenilediği günümüzde parola kullanımı ve SMS doğrulaması bilginin güvenliğini korumaya yetmemektedir. Cep telefonu operatörlerine yapılan bir SIM takas saldırısında çağrı merkezi çalışanları kurbanın cep telefonu numarasını saldırganın SIM kartına atamaya ikna edilmişlerdir [82]. Bu gibi sosyal mühendislik saldırıları SMS doğrulama sisteminin güvenliğini sorgulatmış, kişileri ve kurumları biyometrik sistemleri kullanmaya yöneltmiştir.

Ayırt edici ve inkâr edilemez özellikleriyle kolluk kuvvetlerinin adli soruşturmalardaki vazgeçilmezi olan fizyolojik biyometriler, yine aynı özellikleri

sebebiyle tehdit altındadır. Teknoloji ile birlikte yalnızca güvenlik önlemleri değil anti forensic teknikler de gelişmektedir. 3D yazdırılan kafalar, yüz tanıma sistemleri için hazırlanan maskeler, sentetik irisler ve sahte silikon parmak izleri artık bilim kurgunun konusu değil içinde bulunulan dijital çağın bir gerçeğidir. Biyometrik verilerin ifşa edilmesi, çalınması veya taklit edilmesi milyonlarca kullanıcıyı ömür boyu sürecek mağduriyetlere mahkum edecektir. Biyometrik veri hırsızlığı geri dönüşü olmayan bir kimlik avıdır. Güvenlik şirketleri bu sebeplerden ötürü davranışsal biyometrik teknolojileri yeni güvenlik katmanı olarak güvenlik hizmetlerine eklemeye başlamıştır. Veri toplamanın kolaylığı, düşük maliyetli oluşu, sürücüsüz araç ve akıllı ev *(IoT- Nesnelerin İnterneti Teknolojisi)* kullanımı, kimlik doğrulamadaki güvenilirliği ve başarılı dolandırıcılık tespitleri *(Fraud Analizi)* gibi nedenlerle davranışsal biyometri araştırmaları son yıllarda ivme kazanmıştır.

Davranışsal biyometrik sistemler oda ışığı, ağ/paket trafiği, jeolokasyon, zaman dilimi ve ağ gecikmesi gibi yeni özellikler eklenerek her geçen gün geliştirilmektedir. Bu yeni özelliklerle beraber hareket verilerini tekrarlamak ve taklit etmek oldukça zordur, davranışsal biyometrik sistemleri atlatmak için başkasının kimliğine bürünmek ve bunu sürdürmek gerekir. Veriler ele geçirildiğinde bile ayırt ediciliği düşük olduğundan gerçek bir kimlikle eşleştirme yapabilmek mümkün değildir.

IOT Analytics 2025 yılına kadar 21 milyardan fazla cihazın internete bağlanabileceğini öngörmektedir. [83]. Kişisel ev aletlerinden endüstriyel cihazlara geniş kullanım alanlarına sahip bu akıllı nesnelerin güvenliğini parolalarla sağlamak zafiyetlere ve siber saldırılara açık hâle getirecektir. Bu veriler ışığında, gelecekte davranışsal biyometrik sistemlerin diğer kimlik doğrulama yöntemlerinin yerini alacağını öngörmek zor değildir.

KAYNAKLAR

[1] Stewart, J., M. (2008). CompTIA Security+: Review Guide: Sy0-201

[2] Saleem, K., Abbas, H., Orgun, M. A., Iqbal, W., Aslam, B. (2016). A Survey of Authentication Schemes in Telecare Medicine Information Systems. *Journal of Medical Systems*, 41 (1).

[3] Alqudah, A., A., M., Abushariah, M.,A., M. (2016). Automatic Identity Recognition Using Speech Biometric. *European Scientific Journal*.

[4] Alqudah, A., A., M., Abushariah, M.,A., M. (2016). Automatic Identity Recognition Using Speech Biometric. *European Scientific Journal.*

[5] Yampolskiy, R. V., Govindaraju, V. (2008). Behavioural biometrics: a survey and classification. *Int. J. Biometrics* , 1(1).

[6] Halteren, H. (2004). Linguistic Profiling for Authorship Recognition and Verification. *Proceedings of the 42nd Annual Meeting of the Association for Computational Linguistics*, 21-26.

[7] Schler, J., Mughaz, D. (2003). Text Categorization for Authorship Verification.

[8] Koppel, M., Schler, J. (2004). Authorship verification as a one-class classification problem. *Machine Learning, Proceedings of the Twenty-first International Conference*.

[9] Zhang, C., Wu, X., Niu, Z., Ding, W. (2014). Authorship identification from unstructured texts. *Knowledge-Based Systems*, 66 (99), 111.

[10] Vel, O. D., Anderson, A., Corney, M., Mohay, G. (2001). Mining Email Content for Author Identification Forensics. *Special Section on Data Mining for Intrusion Detection and Threat Analysis.*

[11] Stolfo, S. J., Wang, K., Hershkop, S., Nimeskern, O. (2003). Behavior profiling of email. *Lecture Notes in Computer Science*, 2665.

[12] Varenhost, C. (2004). Passdoodles; a Lightweight Authentication Method.

[13] Al-Zubi, S., Brömme, A. (2003). Using an Active Shape Structural Model for Biometric Sketch Recognition. *Lecture Notes in Computer Science*, 2781, 187-195.

[14] Lyu, S., Rockmore D., Farid, H. (2004). A digital technique for art authentication. *Proceedings of the National Academy of Sciences*, 101(49).

[15] Ilonen, J. (2003). *Keystroke Dynamics. In: Advanced Topics in Information Processing- Lecture* (2003), 03-04.

[16] Monrose, F., Rubin, A. D. (2000). Keystroke dynamics as a biometric for authentication. *Future Generation Computer Systems*, 16(4), 351-359.

[17] Gunetti, D., Picardi, C., Ruffo, G. (2005). Keystroke Analysis of Different Languages: A Case Study. *Advances in Intelligent Data Analysis VI, 6th International Symposium on Intelligent Data Analysis*, 133-144.

[18] Bergadano, F., Gunetti, D., Picardi, C. (2002). User authentication through keystroke dynamics, *ACM Transactions on Information and System Security*.

[19] Palmer, C., Carter, C., Loehr, J., Koopmans, E. (2007). Movement, planning, and music: Motion coordinates of skilled performance. *McGill University.*

[20] Pusara, M., Brodley, C. E. (2004). User re-authentication via mouse movements. *Workshop on Visualization and Data Mining for Computer Security*.

[21] https://www.plurilock.com/ (12 Haziran 2020).

[22] Dao, V. N. P., Vemuri, R. V., Templeton, S. (2000). Profiling users in the UNIX OS environment.

[23] Maxion, R. A., Townsend, T. N. (2002). Masquerade detection using truncated command lines. *International Conference on Dependable Systems and Networks*.

[24] Marin, J., Ragsdale, D., Sirdu, J. (2001). A Hybrid Approach to Profile Creation and Intrusion Detection. *2nd DARPA Information Survivability Conference and Exposition*, 1.

[25] Yeung, D- Y., Ding, Y. (2003). Host-based intrusion detection using dynamic and static behavioral models. *Pattern Recognition*, 36 (1), 229-243.

[26] Tapiador, J., Clark, J. A. (2011). Masquerade mimicry attack detection: A randomised approach. *Computers & Security*, 30 (5), 297-310.

[27] Mukhopadhyay, D., Banerjee, S. (2006). User Profiling for Host Based Anomaly Intrusion Detection in Windows NT. *First International Conference on Emerging Applications of IT.*

[28] Garg, A., Rahalkar, R., Upadhyaya, S., Kwiat, K. (2006). Profiling Users in GUI Based Systems for Masquerade Detection. *Information Assurance Workshop, IEEE.*

[29] Luettin, J., Thacker, N. A., Beet, S. W. (1996). Speaker identification by lipreading. *Spoken Language, Proceedings., Fourth International Conference*, 1.

[30] Mok, L. L., Lau, W. H., Leung, S., Wang, S. (2004). Person authentication using ASM based lip shape and intensity information. *International Conference on Image Processing*, 1, 561 – 564.

[31] Wark, T., Thambiratnam, D., Sridharan, S. (1998). Person authentication using lip information. *10th Annual Conference Speech and Image Technologies for Computing and Telecommunications*, 1.

[32] Westeyn, T. L., Starner, T. (2004). Recognizing Song- Based Blink Patterns: *Applications for Restricted and Universal Access*, 5, 17-19.

[33] Weaver, J., Mock, K., Hoanca, B. (2011). Gaze-Based Password Authentication through Automatic Clustering of Gaze Points. *IEEE International Conference on Systems, Man, and Cybernetics.*

[34] Kale, A., Cuntoor, N., Rajagopalan, A. N., Krueger, V. (2003). Identification of Humans Using Gait.

[35] Nixon, M. S., Carter, J. N. (2004). On Gait As A Biometric: Progress and Prospects. *European Association for Signal Processing.*

[36] Connor, P., Ross, A. (2018). Biometric recognition by gait: A survey of modalities and features. *Computer Vision and Image Understanding*, 167, 1–27.

[37] Georgiou, T. (2018). Rhythmic Haptic Cueing for Gait Rehabilitation of Hemiparetic Stroke and Brain Injury Survivors.

[38] Şişli, H., Şahin, M. (2014). Gait Analysis. https://slideplayer.biz.tr/slide/2021363/ (10 Haziran 2020)

[39] Pamudurthy, S., Guan, E., Mueller, K., Rafailovich, M. (2005). Dynamic Approach for Face Recognition Using Digital Image Skin Correlation. *Lecture Notes in Computer Science*, 3546, 1010-1018.

[40] Mainguet, J-F. (2006). Biometrics.

[41] Trujillo, M.O., Shakra, I., El-Saddik, A. (2005). Haptic: the new biometrics-embedded media to recognizing and quantifying human patterns. *Proceedings of the 13th ACM International Conference on Multimedia.*

[42] Chuda, D., Burda, K. (2016). Toward Posture Recognition with Touch Screen Biometrics. *International Conference on Computer Systems and Technologies - CompSysTech'16*.

[43] Julita, A., Salehuddin, F., Azlina, O., Haroon, H., Mardiana, B., Manap, Z. (2009). Online Signature Verification system. *IEEE Colloquium on Signal Processing*.

[44] Sabancı University Biometrics Research Group. https://biometrics.sabanciuniv.edu/signature.html_ (10 Haziran 2020)

[45] Mujahed, J., Al- Najdawi, N., Tedmari, S. (2014). Offline handwritten signature verification system using a supervised neural network approach. *2014 6th International Conference on Computer Science and Information Technology.*

[46] Muralidharan, N., Wunnava, S. (2004) Signature verification: a popular biometric technology. *Second LACCEI International Latin American and Caribbean Conference for Engineering and Technology*.

[47] Schomaker, L. (2008). Writer Identification and Verification. *Advances in Biometrics: Sensors, Algorithms and Systems*, 247-264.

[48] Ballard, L., Lopresti, D., Monrose, F. (2006). Evaluating the Security of Handwriting Biometrics.

[49] Zhu, Y., Tan, T., Wang, Y. (2000). Biometric Personal Identification Based on Handwritin.

[50] Ratha, N.K., Senior, A., Bolle, R. M. (2001). Automated biometrics. *Proceedings of International Conference on Advances in Pattern Recognition.*

[51] Campbell, J. P. (1997). Speaker recognition: a tutorial. *Proceedings of the IEEE*, 85 (9), 1437-1462.

[52] Ciota, Z. (2004). Speaker verification for multimedia application. Systems, Man and Cybernetics, *2004 IEEE International Conference*, (3). doi: 10.1109/ICSMC.2004.1400748 (10 Haziran 2020).

[53] Key, B., Neal, K., Frazier, S. (2006). The Use of Biometrics in Education Technology Assessment. *Ball State University*.

[54] Deshpande, S., Chikkerur, S., Govindaraju, V. (2005). Accent classification in speech. *Fourth IEEE Workshop on Automatic Identification Advanced Technologies* (AutoID'05). doi: 10.1109/AUTOID.2005.10 (10 Haziran 2020).

[55] Lin, X., Simske, S. J. (2004). Phoneme-less hierarchical accent classification. Signals, Systems and Computers. *Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers*. doi: 10.1109/ACSSC.2004.1399473 (10 Haziran 2020).

[56] Wang, X., Ito, A., Suzuki, M., Makino, S. (2005). Smile and laughter recognition using speech processing and face recognition from conversation video. 2005 *International Conference on Cyberworlds*.

[57] Wang, H- M., Tsai, W- H. (2005). Automatic singer recognition of popular music recordings via estimation and modeling of solo vocal signals. *IEEE Transactions on Audio, Speech, and Language Processing*, 14(1), 330-341.

[58] Jain, A. K., Dass, S. C., Nandakumar, K. (2004). Can soft biometric traits assist user recognition?. *Proceedings of SPIE - The International Society for Optical Engineering*, 5404.

[59] Liu, A., Salvucci, D. (2001). Modeling and Prediction of Human Driver Behavior. *In: Proc. 9th International Conf. Human-Computer Interaction*. (2001)

[60] Inata, K., Raksincharoensak, P., Nagai, M. (2008). Driver behavior modeling based on database of personal mobility driving in urban area. *International Conference on Control, Automation and Systems.*

[61] Salvucci D., Mandalia, H.M., Kuge, N., Yamamura, T. (2007). Lane- Change Detection Using a Computational Driver Model. *Human Factors The Journal of the Human Factors and Ergonomics Society.*

[62] Yampolskiy, R., Govindaraju, V. (2006). Use of behavioral biometrics in intrusion detection and online gaming - art. *Proceedings of SPIE - The International Society for Optical Engineering*, 6202.

[63] Jansen, A.R., Dowe, D.L., Graham, E.F. (2000). Inductive Inference of Chess Player Strategy. *PRICAI 2000 Topics in Artificial Intelligence: 6th Pacific Rim International Conference on Artificial Intelligence.*

[64] Phua, C., Lee, V. (2010). A Comprehensive Survey of Data Mining- based Fraud Detection.

[65] Fawcett, T. (1997). Adaptive Fraud Detection. *Data Mining and Knowledge Discovery*, 1(3), 291-316.

[66] Hilas, C.S., Sahalos, J.N. (2005). User profiling for fraud detection in telecommunication networks.

[67] Spafford, E. H., Weeber, S. A. (1993). Software forensics: Can we track code to its authors?. *Computers & Security*, 12(6), 585-595.

[68] Frantzeskou, G., Gritzalis, S., MacDonell, S. G. (2004). Source Code Authorship Analysis for Supporting the Cybercrime Investigation Process. *Proceedings of the First International Conference on E-Business and Telecommunication Networks*.

[69] Jain, A. K., Pankanti, S., Hang, L. (2008). *Biometric Identification. Information Systems Security*, 43(2), 90-98.

[70] Hsiao, A., Moffatt, K. (2019). Know Which MFA Technologies to Avoid—and Which to Embrace. https://www.plurilock.com/blog/know-which-mfa-technologies-to-avoid-and-which-to-embrace/ (10 Haziran 2020).

[71] Gupta, S., Rogers, M. (2016). Using Computer Behavior Profiles to Differentiate between Users in a Digital Investigation in a Digital Investigation. *Conference on Digital Forensics, Security and Law Proceedings.* (United States v. Moreland-Karar: 14 Aralık 2011, *Amerika Birleşik Devletleri-davacı, Keith Moreland-sanık*)

[72] Davranışsal Biyometri Vaka Çalışmaları. Biocatch https://www.biocatch.com/blog/biometrics-case-studies-in-banking/ (12 Haziran 2020).

[73] Taylor, J. (2019, 14 Ağustos). Major breach found in biometrics system used by banks, UK police and defence firms. *The Guardian.* Erişim adresi: https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms (11 Haziran 2020)

[74] Jain, A. K., Cao, K. (2016). Hacking Mobile Phones Using 2 D Printed Fingerprints. *Department of Computer Science and Engineering Michigan State University Technical Report MSU-CSE-16-2.*

[75] Ramachandra R., Busch, C. (2017). Presentation Attack Detection Methods for Face Recognition Systems: A Comprehensive Survey. *ACM Computing Surveys* (50) 1: 8. https://dl.acm.org/doi/10.1145/3038924 (12 Haziran 2020).

[76] Chawla, S., K., Lamba, V., Jangra, S. (2018). Synthetic Iris as a Vulnerability of Iris Recognition System. *Journal of Image Processing & Pattern Recognition Progress*, 5 (3).

[77] We Are Social 2019 Türkiye'de Medyada Harcanan Zaman İstatistikleri. Global Web Index (Q2 & Q3 2018).

[78] Krausova, A. (2018). Online Behavior Recognition: Can We Consider It Biometric Data under GDPR?. *Masayk University Journal of Law and Technology*, 12 (2): 161. doi: 10.5817/MUJLT2018-2-3. (10 Haziran 2020).

[79] Wake-Up Call on Users' Poor Password Habits- SecureAuth Survey. (2017). *Wakefield Research.* https://www.secureauth.com/sites/default/files/resources/2018-09/180926-CIAM%20Infographic.pdf (12 Haziran 2020).

[80] Yılmaz, H., E.(2016). Rubber Ducky Saldırısı Nedir? https://www.linkedin.com/pulse/rubber-ducky-sald%C4%B1r%C4%B1s%C4%B1-nedir-hasan-emre-yilmaz/?originalSubdomain=tr (10 Haziran 2020)

[81] Average Amount Of Time Spent Per Day Using Social Media (In Hours And Minutes) With Year-On-Year Change. We Are Social- Global Web Index. (2019).

[82] Lee, K., Kaiser, B., Mayer, J., Narayanan, A. (2020). An Empirical Study of Wireless Carrier Authentication for SIM Swaps. *Department of Computer Science and Center for Information Technology Policy Princeton University*. https://www.issms2fasecure.com/assets/sim_swaps-03-25-2020.pdf (10 Haziran 2020).

[83] Symanovich, S. (2019). The future of IoT: 10 predictions about the Internet of Things. https://us.norton.com/internetsecurity-iot-5-predictions-for-the-future-of-iot.html (10 Haziran 2020).

Bölüm 6

BİYOMETRİDE YENİ NESİL DAVRANIŞ MODELLEME YAKLAŞIMLARI, RİSKLER VE ÖNGÖRÜLER

Bilgehan Arslan - Çağla Aksoy - Şeref Sağıroğlu

21. yüzyılın ortasından itibaren her geçen gün bir yenisi ile karşılaştığımız teknolojiler, yaşam tarzımıza muazzam değişiklikler getirmiş ve internet kullanımının tüm dünyada yaygınlaşmasıyla bireylerin giderek daha esnek bir yaşam tarzını benimsemelerine fırsat sunmuştur. Toplumlarda bireyin sürdürdüğü yaşantı ve alışkanlıkların alternatifleri siber dünyada yer bulmuş, mevcut olan alışkanlıklar, yaşam tarzları, davranışlar ve sorunlar da siber dünyaya kaymaya başlamıştır. Bu hususta hep aynı soru akıllara gelmektedir: Bireyin siber dünyada varlığını sürdürürken karşılaşabileceği riskler neler olabilir? Bu sorunun cevabını ararken, siber dünyayı günümüz dünyasına alternatif olarak görülen ve bireysel sorumluluklarımızı daha kolay gerçekleştirebileceğimiz basit hizmetler olarak tanımlarsak hata yapmış oluruz. Nasıl ki sosyal yaşantımız sadece bireysel ihtiyaçlarımızı karşılamak anlamına gelmiyorsa, siber dünyada da gerçekleştirdiğimiz her eylem sadece basit hizmetler olarak görülmemelidir. Yeni dünya düzeninin bir parçası olan bu sanal oluşumların kendine ait kuralları, stratejileri, politikaları, hedefleri ve kendi menfaatlerine hizmet etme amaçları vardır. Kitabın bu bölümünde, siber dünyanın sunduğu hizmetlerden biri olan sosyal medya platformları ve bu platformlarda paylaşılan her türlü içeriğin bireyleri ve toplumları tanımlamak ve anlamlandırmak adına nasıl kullanıldığı üzerinde durulmuştur. Bugüne kadar, özellikle konu sosyal medya platformları olduğunda ilk akla gelen sosyal çevrimiçi ağ ortamlarından elde edilen bilgilere dayanarak bireyleri ve toplumları analiz edebilecek karakteristikler ve bu alanda yapılan çalışmalar, bu bölümde incelenmiştir. İncelenen çalışmalarda kullanılan yöntemler, bu

yöntemlerin birbirlerine göre üstünlükleri ve eksiklikleri detaylı olarak değerlendirilmiştir. Mevcut çalışmalarda yer alan sosyal çevrimiçi ağ ortamındaki birey ve toplumu tanımlayabilme, anlamlandırabilme ve analiz etme amacına yönelik olarak değerlendirmelere de yer verilmiştir.

6.1. GİRİŞ

İnsan düşünen, öğrenen ve kendisini sürekli geliştiren meraklı bir varlıktır. Çevresini anlamaya, öğrenmeye, bilinmezlikleri gidermeye ihtiyaç duymaktadır. Aradığı cevaplar ise kendini ve içinde yaşadığı dünyayı daha iyi anlamak, öğrenmek ve kavramak üzerinedir. Bilimsel ve teknolojik gelişmeler de buna katkılar sağlamaktadır. Şimdiye kadar yapılan çalışmalar, biyoloji alanında genotip ve fenotip özelliklerini tanımlamayı, sinirbilim ve fizyoloji ile insan-bilgisayar ilişkisini geliştirmeyi, yapay zekâ yaklaşımları ile davranışları modellemeyi, biyometri ile fiziksel ve davranışsal özellikleri ayrıştırmayı başarmıştır. Ancak, bireyi tanımlamak adına kullanılabilecek fiziksel karakteristiklerin yanı sıra, politik görüşü, duygu durumu, konuşma tarzı, yürüyüş stili ve konuşma tarzı gibi karakteristikler de mevcuttur. Bireyler fiziksel ortamlarda bu özelliklerinin tümünü kapsayan bir kimliğe sahiptirler ve beraberinde bu özellikleri taşımaktadırlar. Gelişmekte olan teknoloji ile fiziksel ortamın sınırları değişmiş, internet ise de bu sınırların değişmesi ve büyümesinde öncü rol oynamıştır. Dijital ortamdaki insan, fiziksel ortamdaki insanın yansımalarını içermektedir. Dijital ortamdaki bu varoluş sosyal medya etkileşimiyle giderek büyümekte ve siber fiziksel ortamların yaygınlaşmasını kolaylaştırmaktadır.

Siber ortamdaki bu değişim ve dönüşüm biyometri biliminde de kendisini göstermektedir. Bu değişimi daha iyi anlamak ve riskleri görebilmek için yapılan bu inceleme çalışması, klasik davranışsal biyometrik özelliklerle birlikte bunların dışında kalan bireyi ve toplumu ayırt ve analiz etmeye yarayan özelliklere yoğunlaşmaktadır.

Biyometrik teknolojilerin günümüzde geldiği nokta, bilim kurgu filmlerinde gördüklerimizin ötesine geçmiş durumdadır. Biyometri tabanlı erişim ve kontrol mekanizmaları yüksek güvenilirlikte hizmet ortamı sundukları için sıklıkla tercih edilmektedir. Biyometri tabanlı teknolojilerin temel çalışma prensibi; tanımlama veya doğrulama yapabilmek için her bireyde farklılık

gösteren ve kalıcılığı olan karakteristik özelliklerin toplanabilir olanları ile bireyin eşsizliğini kayıt altına almaktır. Bahsedilen karakteristik özellikler seçilirken dikkat edilmesi gereken hususlar, bu özelliklerin evrensel normlar tarafından kabul edilebilir olması ve bireyi tarif edebilme konusunda yeterli ayrıştırma performansı sağlayabilmesidir. Bugüne kadar parmak izi, yüz, iris, avuç izi, ses, retina, imza, tuş vuruşu vb. karakteristikler biyometrik teknolojilerle birlikte kullanılmıştır. Bahsedilen bu karakteristikler dışında, bireyin fiziksel olarak bünyesinde barındırmadığı fakat tutum ve davranışlarında, kişiliğinde, bilinçli ya da bilinçsiz gerçekleştirdiği her türlü eylemde kendisini diğer bireylerden ayırt edebilmek için kullanılabilecek veri parçacıkları bu bölümün temel konusunu oluşturmaktadır. Bununla birlikte bölümde, yakın gelecekte klasik biyometrik verilerin ve bu bölümde bahsedilen harici verilerin bireyleri tespit ve teşhis etmek dışında hangi amaçlar doğrultusunda kullanılabileceği, bu veriler kullanılarak hangi çıkarımların gerçekleştirilebileceği, çalışmaların getireceği olası riskler ve alınması gerekecek önlemler üzerinde durulmaktadır.

6.2. BİYOMETRİNİN TANIMI, TARİHÇESİ VE GELİŞİM SÜRECİ

Biyometrik özellikler, bir bireyi diğerinden ayırt edebilen fizyolojik (yüz, parmak izi, iris vb.) veya davranışsal (yürüyüş, ses, imza vb.) özellikler olarak tanımlanabilir. Biyometrik özelliklerin belirli bir zaman içerisinde benzersiz ve kalıcı olması güvenilirlik niteliğini de beraberinde getirmektedir [1]. Biyolojik bir ölçümü biyometri olarak belirleyen evrensellik, farklılık, kalıcılık, toplanabilirlik, nicel olarak ölçülebilirlik, performans, kabul edilebilirlik, sahtekârlığa karşı dayanıklılık gibi faktörlerdir [2]. Biyometrinin en genel itibariyle tanımları [2,3]:

- Bir kişinin kendine özgü bir dizi tanınabilir ve doğrulanabilir verilere dayanarak tanımlanmasına ve doğrulanmasına olanak tanıyan,
- Benzerliği belirlemek için kişinin biyometrik özelliklerine ilişkin verileri o kişinin biyometrik şablonu veya öznitelik vektörleriyle karşılaştırabilen,
- Biyometrik verilerin kullanıcıdan alındığı, işlendiği ve bir veri tabanında saklandığı bir kalıp tanıma sistemi olup veriyi alma, benzersiz özellikler çıkarma ve haritalandırma bileşenlerinden oluşan ve

- Bireye ait bir biyometrik verinin birçok bireyin kayıtlı olduğu veri tabanı ile eşleştirilerek "Bu kimdir?" sorusuna cevap bulabilen bir çeşit örüntü tanıma sistemidir.

Farklı stratejileri gerçekleştirebilmek adına hem kurumsal hem de bireysel birçok alanda aktif olarak kullanılan akıllı telefonlar, bilgisayarlar vb. cihazlarda görülen kullanım artışı nedeniyle biyometrik sistemlerin yoğun kullanımı son yıllarda ortaya çıkmış gibi görünmesine rağmen, biyometri ve biyometrik teknolojilerin kökleri M.Ö. 500'e kadar uzanmaktadır. İlk olarak 1980'lerde literatürde yerini almaya başlayan biyometri kavramı ve tarihçesine bakıldığında [2,4,8]:

- Sanayi devrimi, şehirlerin hızla büyümesi ve bununla birlikte gelen ticaret arttırıcı yönlü büyüme, bireylerin tanımlanması ve güvenilir ilişkiler kurma ihtiyacı doğurmuştur. Ayrıca bu dönemde bireylerin birbirinden ayırt edilmesinde kullanılan her türlü yaklaşım popülerlik kazanmıştır. Bu sebeple biyometrinin bu yıllarda gelişimi tarihsel bir tesadüften çok elzem ihtiyaçlardan kaynaklanmaktadır.
- Evangelista Purkinje dokuz tür parmak izi şablonundan bahsetmiş fakat bu şablonları bireyleri ayırt edebilecek bir unsur olarak değerlendirmemiştir. 1856 yılında ise Hermann Welcker, parmak izi modellerinin kalıcı olduğunu ifade etmiştir.
- 1863 yılında Paul-Jean Coulier, iyot dumanının kâğıt üzerindeki gizli baskıları ortaya çıkarmaya yardımcı olabileceğini keşfetmiş ve bu baskıların nasıl kalıcı olabileceğini de göstermiştir.
- 1870'lerde ise Henry Faulds parmak izlerinin kişisel tanımlamada kullanılabileceğini göstermiştir. Bunun yanı sıra parmak izleri için önerdiği sınıflandırma yöntemi ise biyometri alanında ses getiren buluşlardan biri olmuştur.
- 1880'lerde suçlu tespiti için kullanılmasının yanı sıra bireyin kimliğini sembolize etmesi sebebiyle bireyler için bir çeşit imza olabileceği düşünülmesi üzerine, biyometri, farklı bilim insanları açısından üzerinde çalışılan konulardan olmuştur. Özellikle Edward Henry'nin parmak izi standartlarını geliştirmek üzere önerdiği Henry sistemi, parmak izinin biyometrik karakteristik olarak kullanılabilmesi için iyi bir sınıflandırma sistemi olarak görülmektedir.

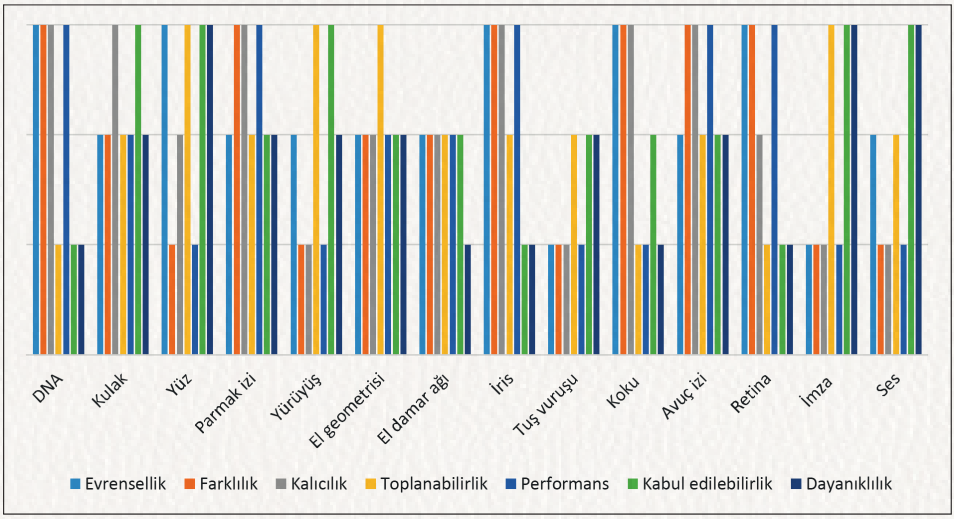
- 1886'da Francis Galton ayrıntılı bir parmak izi analizi ve tanımlama modeli yayınlamış, bu model olay yeri incelemelerinde ve suç tespitinde parmak izlerinin kullanılmasını teşvik etmiş ve parmak izi analizi için istatistiksel bir modelin önerilmesine imkân sunmuştur.
- Bir kişiyi tanımak için biyometrik özelliklerin kullanılması fikri, 1869 yılında İngiltere'de Birleşik Krallık Mükerrer Suçlar Yasası'nın çıkarılmasıyla oluşmuştur. Bu yasa, Birleşik Krallıkta bir suçtan mahkûm olan kişilerin, kimlik kaydının tutulmasını zorunlu hâle getirmiştir. Suçluların kaydedilmesi için parmak izinin kullanılabilirliği üzerinde durulmuştur.
- Biyometrik tanıma kapsamında bilinen ilk araştırma yayını, 1963 yılında Mitchell Trauring tarafından parmak izi eşleşmesi konusunda yayınlanmıştır. 1960'larda ses, yüz ve imza gibi diğer özelliklere dayanan otomatik biyometrik sistemlerin geliştirilmesine de başlanılmıştır.
- Biyometri alanında çığır açan esas gelişmeler 19. yüzyılda gerçekleşmiştir. Bu yüzyıl; parmak izi sınıflandırma sisteminin geliştirilmesi, olay yeri incelemelerinde parmak izi kullanımı ve parmak izi inceleme bürolarının kurulması gibi biyometri alanında bazı önemli atılımlara tanık olmuştur. Biyometrinin gelişimi kronolojik sıra ile incelendiğinde, her yeni buluşun bir sonrakinin gelişimi için ışık tuttuğu görülmektedir. Paris Polis Teşkilatının Kriminal Kimlik Bölüm Şefi olan Alphonse Bertillon, suçluları tespit etmek için bir dizi vücut ölçümü kullanma fikrini geliştirmiş ve uygulamıştır. Kullandığı ölçümler göz rengi, yara izleri gibi literatürde yumuşak (soft) biyometri olarak adlandırılan özelliklerdir. Ancak bu sistem, eksiklikler nedeniyle yerini suçluların parmak izlerini ayırma ve veri tabanına saklama fikrine bırakmıştır.
- Antropolojik ölçümler ilk kez yüz için sonrasında parmak izi ve avuç içi izi için gerçekleştirilmiştir. Sonrasında özellikle parmak izinin farklı uygulama alanlarındaki kullanımının yaygınlaşması, çalışmaların bu alanda odaklanmasına sebebiyet vermiştir.

Yukarıda bahsi geçen ve parmak izi biyometrisi için mihenk taşı görevi yapan buluşlarla birlikte parmak izini oluşturan hatların iyileştirilmesi, parmak izinin suçlu tespitinde kullanılması ve bunu analiz eden büroların kurulması,

parmak izi haricinde yüz, iris, damar tanıma, ses üzerine geliştirilen biyometrik sistemler, bu sistemlerde kullanılan spesifik algoritmalarla biyometri son yıllarda gelişiminin zirvesini yaşamıştır. Yaşanan bu değişim ve gelişim bizlere göstermektedir ki, yeni biyometrik kimlik doğrulama ve tanımlama sistemlerinin geliştirilme olasılıkları tükenmekten çok uzaktır. Biyometrinin gelişimi devam ederken, bu gelişim yapay zekâ ile birleşmekte ve daha yüksek performans sunan sistemler tasarlanabilmektedir. Temel amaç, kullanıcılarını öğrenebilen ve kullanıcılara uyum sağlayabilen biyometrik cihazlar ve sistemler oluşturmaktır. Kesintisiz ve sürekli bir kimlik doğrulama ortamını oluşturmak adına birçok çalışma hâlihazırda sürdürülmektedir. Biyometri daha yaygın hâle geldikçe, tanımlama vekillerinin kullanımı ortadan kalkacaktır. Kendimizi, diğer bir deyişle kendi biyometrik özelliklerimizi, kimliğimizin kanıtı olarak kullanabildiğimiz sistemler günlük hayatımızın bir parçası hâline gelecektir. Günümüzde yüksek güvenilirlik sağlayan sistemlerin geliştirilmesinin yanında bireyi tanımlayabilecek yeni biyometrik özelliklerin keşfi ile de konuya bakış açısı değişimi ve gelişmiş, konuya olan ilgi de çok artmıştır. Bu bölümde, hangi verilerin biyometrik karakteristik özelliklere sahip veriler olarak tanımlandığı, bireyi birbirinden ayırmak için kullanılan verilerin sadece antropolojik temelli olup olmaması gerektiği, yeni özelliklerden faydalanılarak nasıl çözümler geliştirildiği üzerine yapılan çalışmalardan elde edilen sonuçlar detaylı olarak incelenmiş ve konu ile ilgili değerlendirmeler sunulmuştur.

6.3. BİYOMETRİK KARAKTERİSTİKLER VE VERİ TÜRLERİ

Biyometrik özellikler genellikle; özelliklerin beş duyu ile tanımlanabildiği, sonlu ve hesaplanabilir farklılıkların tespitine dayalı fizyolojik biyometri ile insan davranışlarını temel alan davranışsal biyometri olmak üzere iki ana kategoride sınıflandırılır [9]. Bu özelliklerin sürekli bireyleri tanımlamak amacıyla kullanılması için güvenilir, benzersiz, toplanabilir, kullanışlı, uzun vadede değişmeyen, evrensel ve kabul edilebilir olması gerekir [10,11]. Şekil 6.1'de biyometrik modellerde kullanılan biyometrik karakteristiklerin uygulanış biçimleri ve yapısal özellikleri bakımından üstünlükleri ve eksiklikleri verilmiştir. Bu modellerde kullanılan biyometrik karakteristiklerin güvenilirliğini ölçebilmek adına temel kıstaslar belirlenmiştir [2,9]. Bir özelliğin biyometri tabanlı uygulamalarda kullanılabilmesi için belirlenen kıstasların sağlaması durumunda o karakteristiğin bireyi ayırt edici nitelikte olduğu kabul edilmektedir.



Şekil 6.1. Biyometrik Modellerde Kullanılan Karakteristiklerin Uygunluğunun Karşılaştırılması

Fizyolojik biyometri, insan vücudunun doğrudan ölçümü ile ilgilenmekte olup büyük zaman aralıklarında sabit kaldığı düşünülen fizyolojik ölçümleri içermektedir. Davranışsal biyometride ise, insan eylemlerine bağlı karakteristikler ele alınır. Davranışsal biyometriyi fizyolojik biyometriden ayıran en önemli faktör, belirli bir süre zarfında elde edilen ölçümlere dayanması ve davranış kalıplarına odaklanmasıdır [1,12]. Günlük aktivitelerinde farklı davranış örüntülerine sahip olan insanoğlu, pek çok benzersiz beceri, yetenek, duygu durumu, tepki, davranış ve hareket içerisindedir. Bu benzersiz örüntüler, davranışsal biyometrinin de tıpkı fizyolojik biyometri gibi ayırt edici bir özellik olarak kullanılabilmesini mümkün kılmaktadır. Zaman boyutunun davranış imzasının bir parçası olarak dâhil edilmesi, ölçülen davranışın bir başlangıcı, süresi ve bir sonu olması, davranışsal biyometrinin tanımlayıcı özelliklerindendir [12]. Davranışsal biyometri kapsamında psikometri de dâhil olmak üzere farklı disiplinlerden yararlanıldığı, zekâ, yetenek ve kişilik özellikleri gibi psikolojik değişkenlerin ölçümü için nicel testlerin tasarımı, yöntemi ve yorumuyla ilgilenildiği; davranışsal biyometrinin bireylerin profilini çıkarmak ve amaçlarını daha iyi anlamak için kullanıldığı, hedef bir kitlenin ilgisini çekmenin de bunlardan birisi olduğu, kullanım alanlarının her geçen gün artış gösterdiği ve sonuçta bir pazar potansiyeli yaratarak küresel bir boyut kazandığı görülmüştür [13].

Biyometrinin en yaygın uygulama alanı olan kişi doğrulama ve tanımlama sistemlerinde kullanılan davranışsal biyometri türlerinin önemli olanları aşağıda kısaca açıklanmıştır:

- **Yürüyüş Tabanlı Davranış Biyometrisi:** Yürüyüş, dinamik bir davranış biyometrisidir. Uzun bir yürüyüşte meydana gelebilecek vücut ağırlığındaki değişimler ve eklemlerdeki önemli yaralanmalar nedeniyle bu karakteristik değişkendir [14]. Yürüyüş özelliklerine göre bireylerin tanınması 1998 yılında Little ve arkadaşları tarafından önerilmiştir [15]. Yürüme tabanlı sistemler, yürüyen bir kişinin eklemindeki birkaç farklı hareketini ölçmek için video dizisi görüntülerini kullandığından, yoğun işlem gücü gerektirir ve hesaplama açısından maliyetlidir [9]. Yaklaşımın üstünlüğü; uzak mesafeden, düşük çözünürlükte görüntü ile fiziksel temas olmadan veri toplanabilmesidir. Bunlara ek olarak model tabanlı ve görüntü tabanlı yaklaşımlar kullanılması bir diğer avantajıdır [1]. Li ve Yuan sadece yürüyüş tabanlı davranış biyometrisi kullanarak kişi tanıma üzerinde çalışmış, yürüyüş imajlarından elde edilen eksenel mesafeyi, çevre çizgisi genişliğini ve dalgacık özelliğini birleştiren bir yöntem önermiş ve bu sayede kişilerin yürüyüşlerinden kişileri tanıma işlemini gerçekleştirmişlerdir [16]. Sun ve Lo ise giyilebilir sağlık cihazlarıyla güvenli kablosuz iletişimi sağlamak için, yapay sinir ağları tabanlı bir yürüyüş sinyali tahmin algoritmasıyla, sinyal enerji değişimlerini kullanarak yeni bir biyometrik davranış modelleme yaklaşımı önermişlerdir [17].
- **Tuş Vuruş Dinamiği Biyometrisi:** Her bir bireyin klavye kullanması ayırt edici bir özelliktir [9]. Young ve arkadaşları tuş vuruş dinamiğini kullanarak kişilerin kimliklerini doğrulayan bir model önermişlerdir [18]. Bu davranış biyometrisinin her bireye özgü olması beklenemez, ancak kimlik doğrulamasına izin vermek için yeterli eleyici bilgi sunduğu belirtilmektedir [9]. Kimlik doğrulama metin bağımlı ya da metin bağımsız yapılabilmektedir. Bu biyometri, ardışık tuş vuruşları arasındaki süreler, tuş vuruş arası gecikme süresi, tuş vuruşları arasındaki zaman süreleri, bekleme süreleri (yani bir tuşa basılan süre), genel yazma hızı, hataların sıklığı gibi özellikleri kullanır [1]. Bazı bireyler için tipik yazma modellerinde büyük farklılıklar gözlemlenebilmektedir. Bir sistemi kullanan kişinin tuş vuruşları, o kişi bil-

giyi girerken gizlice izlenebilir [9]. Alves ve çalışma grubu, tuş vuruş dinamiği ile kimlik doğrulama işlemini gerçekleştiren bir çözüm sunmuşlardır [19]. Kimlik tanıma ve doğrulama alanı dışında, Tsimperidis ve arkadaşları sadece tuş vuruşu dinamiği ile kişilerin eğitim seviyesini tahmin eden bir model geliştirmişlerdir [20].

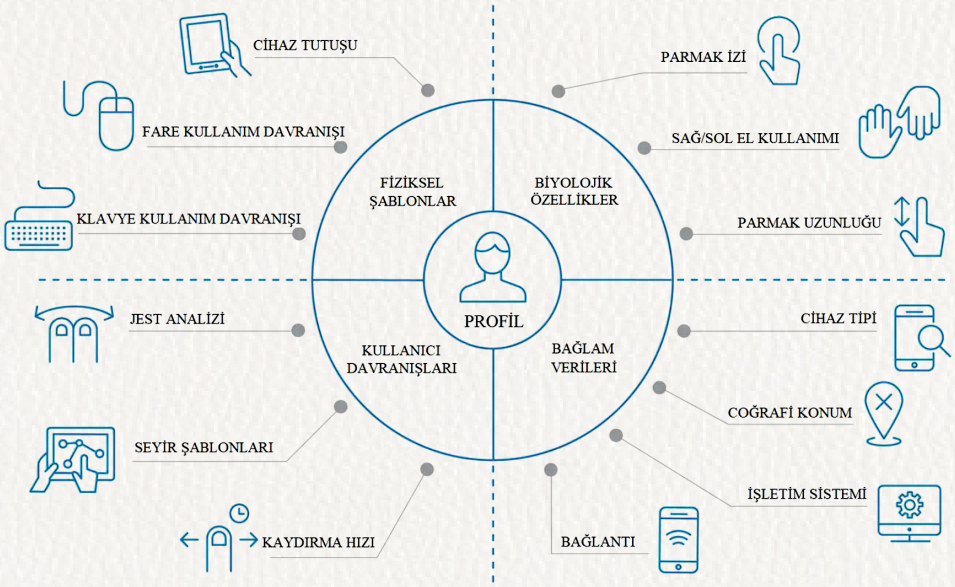
- **Fare Dinamiği Biyometrisi:** Fare özellikleri genel hareket, sürükle-bırak, hareketsizlik, işaret et-tıklat (tek veya çift) eylemlerini kapsamaktadır [1]. Fare dinamikleri, bireysel kullanıcıları fare işletim davranışlarına göre tanımlama sürecidir [21]. Fare kimlik doğrulaması kayıt aşamasını ve giriş aşamasını içerir. Kayıt sırasında yakalanan fare özellikleri kullanılarak bir şablon oluşturulur. Aynı şablon, fare tarafından yakalanan giriş bilgileriyle karşılaştırılır. Fare hassasiyeti performansı etkilemektedir [1]. Davranışsal değişiklik nedeniyle doğruluk düzeyi değişkendir [21]. Fare dinamiği davranış biyometrisi olarak ilk kez Ahmed ve Traore tarafından kullanıcı davranışını modellemek ve kullanıcıyı tanımak amaçlı kullanılmıştır [22]. Shen ve arkadaşları, sadece fare dinamiği davranış ölçümleri ile tek sınıflı destek vektör sınıflandırması kullanarak kullanıcı doğrulama modeli önermişlerdir [23]. Cai ve arkadaşları sürekli kimlik doğrulamada fare dinamiği davranış biyometrisini kullanarak, fare dinamiğindeki davranışsal değişkenliği azaltmak için boyutsallık azaltma yöntemlerini (Çok Boyutlu Ölçeklendirme, Laplace Eigenmap, İzometrik Özellik Haritalama ve Yerel Doğrusal Yerleştirme) kullanan birleşik bir çerçeve önermişlerdir. Kimlik doğrulama görevini gerçekleştirmek için ise dönüştürülmüş özellik alanına ait sınıflandırma tekniklerinden (Rastgele Orman, Destek Vektör Makinesi, Sinir Ağı ve En Yakın Komşu) faydalanmışlardır [21].
- **Konuşma Tanıma Biyometri:** Ses üretimi ağız, burun ve boğazın fiziksel yönlerini göz önüne alsa da bu karakteristik, davranışsal biyometri türü olarak kabul edilmektedir. Çünkü telaffuz ve konuşma şekli, özünde davranışsal özelliklerdir [1]. Konuşmacı kimlik doğrulaması, konuşma dalgalarına dâhil edilen bireysel bilgiler temelinde kimin konuştuğunu otomatik olarak tanıma işlemidir, metin bağımlı ve metin bağımsız olmak üzere iki farklı durumda değerlendirilmektedir [24]. Metine bağlı durumda, biyometrik sistem tarafından kullanıcının belirli bir cümleyi telaffuz etmesi istenirken; metinden

bağımsız durumda, kullanıcının kendi istediği cümleyi telaffuz etmesi beklenmektedir. Hastalıklar, duygusal veya zihinsel durum, hatta yaş gibi çeşitli faktörler nedeniyle hatalı sonuçlar elde edilebilir [1]. Mason ve Brand, dudak şekline dayalı fizyolojik biyometri ve dudak hareketine dayalı davranışsal biyometri kullanarak, Ayrık Kosinüs Dönüşümü metoduyla dudak profili oluşturmuş ve kişi tanıma işlemi gerçekleştirmişlerdir [25]. Maduranga ve arkadaşları, Hidden Markov Model yöntemi temelli metinden bağımsız bir ses kimlik doğrulama sistemi geliştirmişlerdir. Kişilerin ham sesleri yerine ses baskısını saklamışlar ve bunu kimlik doğrulama için kullanmışlardır. [24]. Mahesh ve Swamy avuç içi geometrisi ve konuşma sinyali biyometrilerini birleştirerek, 2 Boyutlu Ayrık Dalgacık Dönüşümü ve Ağırlıklı Öklid Mesafesi metoduyla kişi tanıma işlemini gerçekleştirmişlerdir [26]. Kaur ve arkadaşları yaptıkları çalışmada, konuşma ve imza davranış biyometrilerini birleştirerek kişinin tanıması için bir yöntem önermişlerdir [27].

- **Kişisel Estetik Biyometrisi:** Lovato ve arkadaşları tarafından, kişisel estetik biyometrisinin bireyleri birbirinden ayıran bir özellik olarak davranış biyometrisi kapsamına girdiği deneysel sonuçlarla ispat edilmiş ve literatürdeki yerini almıştır. Çalışmalardaki ana fikir, bir görüntünün takdirini düzenleyen bilişsel mekanizmaların kişisel ve benzersiz olması ve bunların yumuşak biyometrik özellik sağlayabilmesidir. Yaptıkları çalışma ile 200 kullanıcı grubundan, kişisel estetik ile asıl kullanıcıyı yüksek hassasiyetle ayırt edebilmişlerdir [28]. Cinsiyet tahmininin bireyin kişisel estetik tercihleri ile yapılabileceği, ilk defa 2016 yılında Azam ve Gavrilova tarafından öne sürülmüştür. Çalışmalarında destek vektör makinesi, en yakın komşu ve karar ağacı sınıflandırma yöntemlerini kullanılmışlardır. 24.000 imajın 120 Flickr kullanıcısına sunularak yapılan deneylerde %77'lik bir doğru cinsiyet tahmin oranı elde edilmiştir [29]. Sieu ve Gavrilova ilk defa, gen ifade programlama yöntemini kişisel estetik tercihleri üzerinde uygulanarak birey kimlik tanıması yapmıştır. Kullanılan yöntemle özellik boyutu düşürülmüş, doğruluk oranı arttırılmış ve hesaplama süresi azaltılmıştır. Deneyler, 40.000 imaj 200 Flickr kullanıcısı ile gerçekleştirilmiş olup %94 doğruluk oranıyla kimlik tanıma başarısı ilde edilmiştir [30].

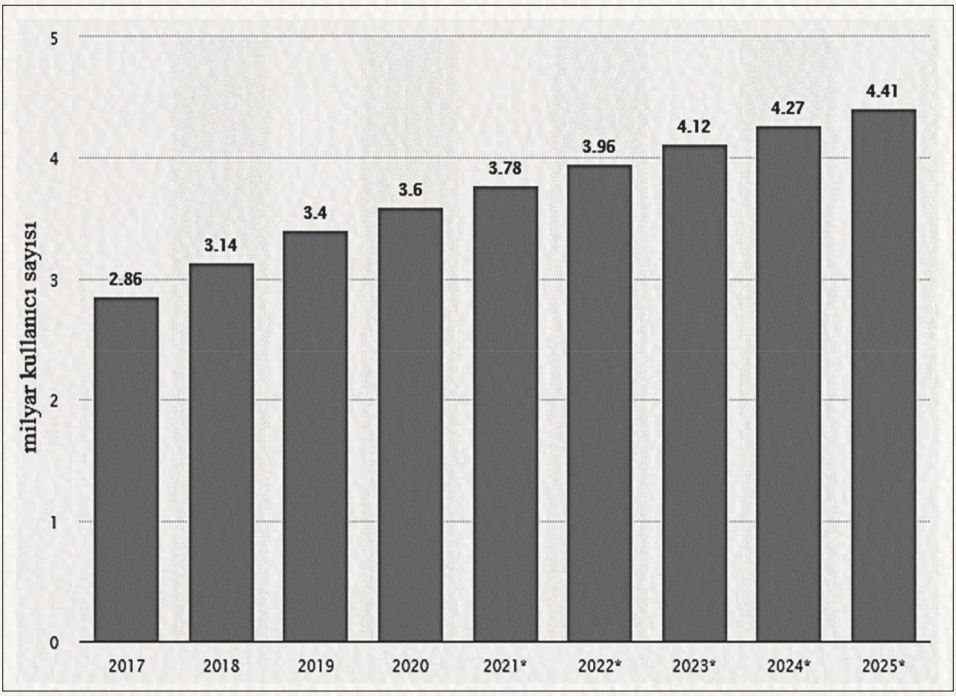
- **Yazılım-İnsan Etkileşimi Tabanlı Davranış Biyometrisi:** Bu davranış biyometrisi kendi içerisinde beş kısımda sınıflandırılmaktadır.
  - E-posta gönderme davranışında; e-posta uzunluğu, gelen kutusunun boşaltılma sıklığı, yazışma sıklığı, boyut gibi özellikler bir bireyin davranışsal profilini oluşturmak için kullanılmaktadır [31,32].
  - Programlama stilinde; belirli bir kod parçasından asıl yazarın kim olduğunun bilinmesi sağlanabilir [32].
  - Bilgisayar oyun oynama stratejisinde; her oyuncunun davranış profillerini çıkarmak için özel bir yazılım tasarlama, her oyuncu için bir profil imzası üretme, kimlik doğrulama gibi çözümler geliştirilmiştir [32,33,34].
  - Biyometrik taslak ile kullanıcıların yalnızca önceden kimliği doğrulanmış kullanıcı tarafından kullanılabilen taslak hakkındaki bilgileri ölçülmektedir [32].
  - Komut satırında; işletim sistemi ile etkileşimde bulunan kullanıcının kullandığı komut setini profilleme yapılmaktadır [32].
- **El Yazısı Biyometrisi:** Yazar tanımlama ve doğrulama tekniği 1990'lı yıllarda gelişmeye başlamıştır [35]. Tian ve arkadaşları, kullanıcıların şifrelerini üç boyutlu (3B) bir alanda girdirerek, kısa ve kolay kırılan şifrelerin davranışsal biyometriye yani 3B imzalara dönüştürülmesini sağlamışlardır [36].
- **Hobi/Alışkanlık Temelli Davranış Biyometrisi:** Jiang ve arkadaşları, kişilerin hobilerinden elde edilen alışkanlık temelli davranışsal biyometriye dayalı yeni bir kullanıcı kimlik doğrulama tekniği sunmuşlardır [37].
- **Göz Hareketleri ve Odaklanma Biyometrisi:** Rigas ve arkadaşları göz hareketleri ve odaklanmasına dayalı göz hareketi biyometrisi üzerine önerilerde bulunmuşlardır. Deneklerin göz hareketleri izlenerek, yüz görüntüleri kayıt altına alınarak ve her katılımcının dikkat noktaları hakkında veriler toplanarak dikkatleri ölçülmüştür [38]. Juhola ve arkadaşları ise göz hareketi biyometrisinde düzensiz göz hareketlerini kullanarak bir doğrulama yöntemi önermişlerdir [39].
- **Dokunmatik Ekran ve Akıllı Cihaz Etkileşim Biyometrisi:** Son yıllarda sayısı hızla artan dokunmatik akıllı cihazlar üzerine de pek çok çalışma yapılmıştır. Kullanılan cihazların dokunmatik ek-

ranlarına dokunma hareketleri, hafifçe dokunma, kaydırma veya çoklu dokunma gibi davranışlarının ayırt edici bir kullanıcı davranışı olduğu [40], dokunmatik ekranda hem parmak hem ekran kalemi etkileşimi [41], giyilebilir gözlüklerde dokunma ve ses biyometrisi kullanılarak kullanıcıların sürekli doğrulanması [42], akıllı telefonlarda kaydırma işlemleri ve hareket dinamikleri ile doğrulama [43], hem telefona ilk girişte hem de girildikten sonra ekrana dokunma dinamiklerinin birlikte kullanılabileceği bir kimlik doğrulama sistemi önerisi [44], dokunmatik tuşlar ile yapılan dokunma testleri ile klasik tuş vuruş sistemlerinde kullanılan tipik özniteliklerin yanı sıra, hız ve uzaklığın da kullanılarak doğrulama yapılması [45], ekranlara çoklu dokunuş özelliklerinin zaman serisi olarak ele alınması [46] ve son olarak dokunmatik ekran ile kullanıcı arasındaki etkileşimde oluşan 30 farklı davranışsal biyometrik özniteliğin çıkarılarak doğrulama işlemlerinde kullanılmasını [47] kapsayan pek çok çalışma mevcuttur. Bu alandaki çalışmaların kapsamının daha iyi anlaşılması için ilgili bir resim Şekil 6.2'de verilmiştir.

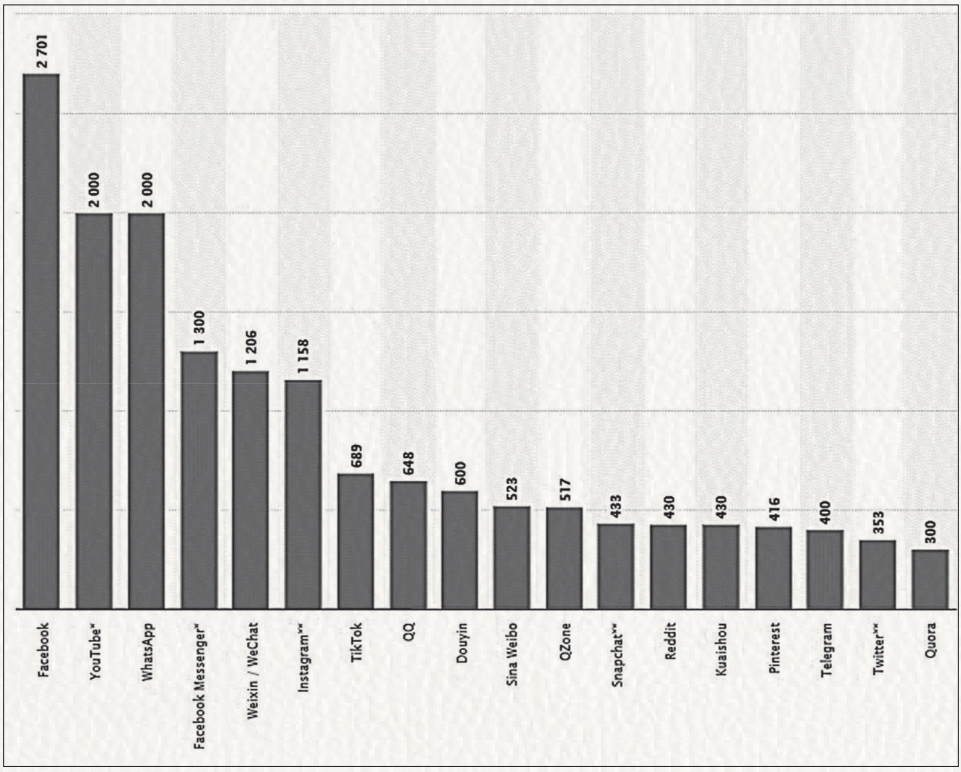


Şekil 6.2. Akıllı Cihazlarda Biyometrik Davranış Temelli Profilleme ([48] nolu kaynaktan Türkçeleştirilmiştir).

- **Sosyal Davranış Biyometrisi:** Bu davranış biyometrisinde en etkili ortam sosyal ağ ve medya platformları gibi elektronik ortamlardır. Küresel internet kullanıcılarının sayısının hızla arttığı dünyamızda kullanıcılar, günde yaklaşık 136 dakika sosyal ağ kullanmaktadırlar. Dünya çapında aktif sosyal medya kullanıcı sayısı 2018'de yaklaşık 3,14 milyar iken, 2021 yılına kadar bu sayının aylık 3,78 milyara ulaşması beklenmektedir. Bu da dünya nüfusunun yaklaşık üçte birini oluşturmaktadır [49]. Bu muazzam artış, sosyal medyanın bireylerin ve toplumların hayatlarında büyük bir yer kapladığını ve bunun gelecekte daha da artacağını göstermektedir. Şekil 6.3'te dünya genelinde 2010 ve 2021 yılları arasındaki sosyal ağ kullanım sayıları Şekil 6.4'te ise 2020 Ekim ayı itibariyle dünyada en çok kullanılan sosyal medya uygulamalarının dağılımı görülmektedir. Bu husus daha detaylı olarak Bölüm 6.4'te açıklanacaktır.



Şekil 6.3. Statista verilerine göre 2010 ve 2021 yıllarındaki sosyal ağ kullanıcıları miktarı [49]



Şekil 6.4. Statista verilerine göre 2020 Ekim ayı itibariyle dünyada en çok kullanılan sosyal medya uygulamaların dağılımı [50]

6.4. SOSYAL DAVRANIŞ BİYOMETRİKLERİ VE YUMUŞAK BİYOMETRİKLER

Yumuşak biyometri kişinin vücudundan (boy, yaş, deri ve saç rengi, kilo, yürüyüş, yüz ifadeleri ve dokusu, etnik köken, dudak hareketleri vb.) elde edilen verilere dayalı analiz sonucunda kimlik doğrulama veya kişileri belirleme çalışmalarını kapsamaktadır. Bu hususta iki temel etik konu gündeme gelmektedir [51,52]:

- Yumuşak biyometrik özelliklerin bazıları güçlü bir etnik bilgiyi bünyesinde barındırır.
- Yumuşak biyometri insanların sınıflandırılması ve profillenmesi için güçlü bir potansiyele sahiptir, bu nedenle bireyleri damgalama ve dışlama süreçlerini destekleme riski vardır.

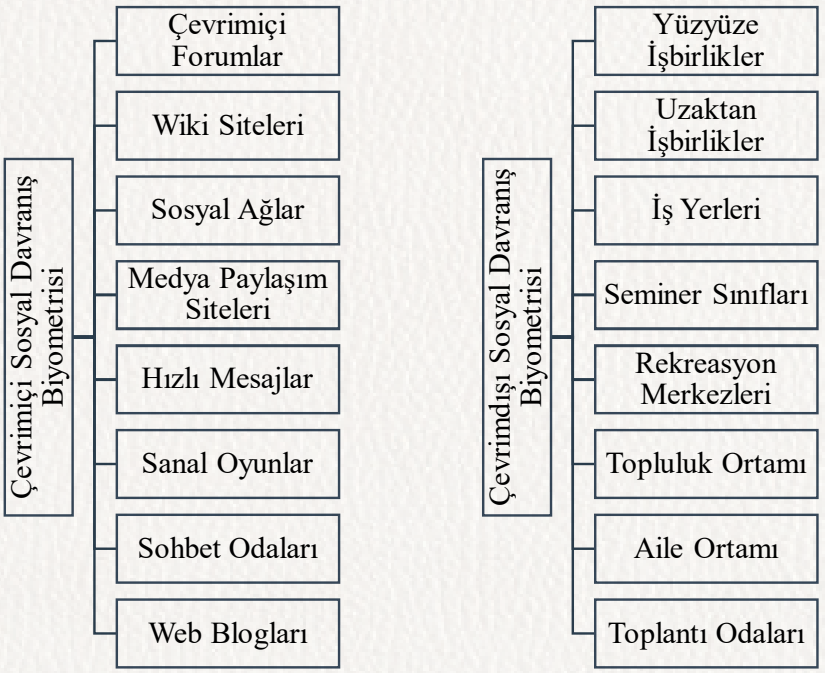
Bertillon tarafından geliştirilen ilk kişisel tanımlama sistemi üç ölçüt üzerinden yapılmaktadır. Bu ölçütler; antropometrik ölçümler, morfolojik ölçümler ve doğuştan ya da sonradan oluşan anomalilerdir [53]. Bu ölçütlerin kalıcı olmaması, birden fazla kişide benzerlik gösterebilmesi ve yüksek hata oranına sahip olması sebebiyle bireyi sadece sınırlı bir doğrulukla tanımlayabilmektedir. Bu sebeple, geleneksel biyometrik sistemlerin performansını arttırmak için yumuşak (soft) biyometrik özellikler kullanılmaktadır. Yumuşak biyometrik özelliklerin, bireylerin doğrudan tanımlanabilmesi için yeterli olmadığı düşünülmesinden dolayı bu özellikler, bireyler tarafından rahatlıkla birçok farklı sosyal ağ platformlarında paylaşılmaktadır. Fakat asıl risk; tek başına ayırt ediciliği yetersiz olan bu tür verilerin, günümüz teknolojileri ile değerlendirildiğinde büyük bir biyometrik veri tabanını filtreleyerek olası ihtimalleri asgariye indirmek, hatta başka sınıflandırma etkisine sahip bileşenlerle birlikte değerlendirildiğinde bireyi doğrudan tespit edebilecek güç ve yeterlilikte oluşudur.

Sosyal davranış biyometrisi ise kişinin günlük faaliyetlerini, bağlantılarını, bağlantı şekillerini, kullanım sıklıklarını vb. sosyal davranış örüntülerini kapsar. Şekil 6.3 ve Şekil 6.4'teki verilerde de belirtildiği üzere sosyal ağların kullanımı ve bu ağların bireylerin hayatındaki öneminin artması da bu konuda pek çok çalışma yapılmasının önünü açmıştır. Sultana ve arkadaşları tarafından, bir kişinin sosyal ağ bağlantılarının, mekânsal-zamansal bilgi, etkileşim tarzı gibi sosyal davranış biçimini tanımlamak için iyi bir bilgi kaynağı olabileceği hipotezine dayanılarak, kişi tanıma ve doğrulama amacıyla ilk defa sosyal davranış biyometrisi olarak adlandırılan yeni bir tür davranışsal biyometri tanıtılmış ve bu amacı gerçekleştirmek için bir çerçeve önerilmiştir [54].

Sosyal davranış biyometrisi, Şekil 6.5'ten görülebileceği gibi çevrimiçi ve/veya çevrimdışı olarak çok farklı ortamlardan, mekânlardan, web sitelerinden, uygulamalardan veya sistemlerden elde edilebilmektedir. Hesaplamalı sosyal bilimler ve sosyal bilişim gibi büyük umut vaat eden disiplinler arası veya çok disiplinli çalışmalar, bireyi doğrudan tanımlamak ya da tanımlamaya yardımcı olmak için kullanılacak biyometrik karakteristikler haricinde yeni veri kaynaklarının varlığını da ortaya koymuştur [55]. Gerçek dünyada dış görünüşü, sesi, tutum ve davranışı, hareketi ve karakteri ile diğerlerinden farklılaşan birey, sanal dünyada ise sosyal ağ platformlarda yapılan paylaşımlar, ilgi alanına giren web sayfaları, takip edilen kişiler ve dijital ortamlarda kayıt altına alınmış her türlü eylem gibi farklı kritik verilerle birbirinden ayrışabilmektedir (Şekil 6.5).

Sosyal davranış biyometrisi üzerine yapılan çalışmalarda;

- Sultana ve arkadaşları, çevrimiçi sosyal ağlardan biri olan Twitter uygulamasındaki kullanıcıların sosyal etkileşimlerini, sosyal davranışsal biyometrik özellik çıkarılması için analiz etmişlerdir. Analiz için haftada 100'den fazla tweet paylaşan 50 kullanıcının 4 aylık verisini toplamışlardır. Yapmış oldukları çalışmada bireylerin sosyal ağ faaliyetlerinde ayırt edici davranış kalıplarının bulunduğunu deneysel sonuçlarla elde etmişlerdir. Çalışma sonucunda, kişi kimlik doğrulaması için Twitter tabanlı sosyal davranış biyometrisi özelliklerinin kullanılmasının mümkün olabileceğini göstermektedirler [56].
- Aynı çalışma grubu, 241 Twitter kullanıcısının çevrimiçi sosyal ağ etkileşimlerinden bir dizi sosyal davranış özelliği tanımlamış ve bu özellikleri kullanarak kullanıcı tanıma işlemi için bir çerçeve önermiştir. Ayrıca sadece son 10 tweetin bireylerin veri tabanındaki kullanıcıların %58'ini tanıması için yeterli olduğunu ispatlamışlardır [57].



Şekil 6.5. Çevrimiçi Sosyal Davranışsal Biyometrik Alan Uygulamaları (a), Çevrimdışı Sosyal Davranışsal Biyometrik Domain Uygulamaları (b) [58]

- Sultana ve Gavrilova, Twitter uygulamasını temel alarak yaptıkları çalışmada, her bir kullanıcı için her oturumdaki paylaşımlarının (orijinal tweeti, reply, mention retweet) zaman damgasını ayrıştırmışlardır. Zaman damgaları dışındaki veriler (konum, zaman dilimi, hashtagler, weblinkler vb.) göz ardı edilmiştir. Kullanıcıların zamansal profillerini oluşturarak, benzerlik ölçümlerini ve füzyon puanlarını hesaplamışlardır. Böylelikle zamansal verilerin yeterli davranış biyometrisi özelliği içerdiğini ve bu özelliklerin kullanılarak kimlik doğrulama işleminin gerçekleştirilebileceğini deneysel sonuçlarla ispatlamışlardır [58].
- David Delgado-Gomez ve arkadaşları kişilik özelliklerinin bir biyometrik model olarak kullanılabileceğini önermişlerdir. Çalışmada 724 kişiye anket uygulamışlardır. Ankette, psikolojik alanda yaygın olarak büyük beşli olarak bilinen beş farklı kişilik özelliğinin ölçülmesi amaçlanmıştır. Kişilik özellikleri, Samejima'nın modeli kullanılarak tahmin edilip, daha sonra bireyleri ayırt etmek için kullanılmıştır [59].
- Golbeck ve arkadaşları, bir kullanıcının beş faktör kişilik özelliklerinin Twitter'da paylaştıkları genel bilgilerden tahmin edilebileceğini, makine öğrenme algoritması olan ZeroR ve Gaussian Prosesler kullanarak göstermişlerdir. Geliştirdikleri yöntemde beş faktör kişilik özelliklerinin belirlenmesi için kullanıcıların paylaşımlarındaki kelimeleri incelemişlerdir [60]. Ayrıca, Golbeck ve arkadaşları bir kullanıcının beş faktör kişilik özelliklerinin, Facebook'ta paylaştıkları genel bilgilerden (Facebook profil verileri, arkadaş sayıları, ağ yoğunluğu gibi özellikleriyle) makine öğrenmesi yöntemiyle tahmin edilebileceğini göstermişlerdir. Bu çalışmalarda, dilbilgisi sorgulama ve kelime sayısı uygulamasından faydalanılmıştır [61].
- Adalı ve Golbeck; Twitter uygulaması üzerinde, sosyal davranıştan yola çıkarak, beş faktör kişilik özelliklerini belirleme işlemini ZeroR, Gaussian Process ve Weka kullanarak gerçekleştirmişlerdir. Bu çalışmada diğerlerinden farklı olarak sosyal medya kullanım yoğunluğu, kullanılan mesaj içeriği (link, hashtag vb.), takipçi ve arkadaş etkileşimi, sosyal medya etkileşimin karşılıklı olması gibi harici sosyal davranış ölçümlerini kullanmışlardır [62].
- Kalghatgi ve çalışma grubu, Twitter verileri üzerinde, beş faktör modeline dayanarak ve dilsel özellik kullanarak, sinir ağları yöntemiyle

kişilik tahmini gerçekleştirmişlerdir. Bu çalışmada beş faktör modeli ayrıntılı bir şekilde açıklanmıştır [63].

- Gu ve arkadaşları, çevrimiçi bir sosyal ağ olan Sina Weibo uygulaması ile mikroblog paylaşımları ve diğer sosyal davranışlar kullanılarak beş faktör modeline dayalı kullanıcı kişilik özelliklerini incelenmişlerdir [65].
- Lien ve arkadaşları, basit denetimli öğrenme algoritmaları ile günlükleri (bir kullanıcının her ziyaret edilen URL'si) kaydedilmemiş olsa bile, kullanıcının göz atma günlüklerinden türetilen özelliklere dayalı olarak bir kullanıcının kişiliğini ve demografik bilgilerini (yaş, cinsiyet ve ilişki durumu) tahmin etmeyi başarmışlardır. Kullanıcı kişiliğini ise altı faktör modeli (dürüstlük-tevazu, nevrotizm, dışa dönüklük, uyumluluk, disiplinlilik, yeniliklere açıklık) kullanarak oluşturmuşlardır [65].

6.5. SONUÇ VE DEĞERLENDİRMELER

Biyometrik sistemler hem kamu alanında hem de özel sektörde; biyometrik tanıma aracı, fiziksel tesislere ve finansal hesaplara erişim sistemi, yerel bakış açısıyla suçlu/küresel bakış açısıyla teröristlerin tespiti, sağlık ve sosyal hizmetlerin kişiselleştirilmesi gibi birçok farklı hizmeti sağlamak adına kullanılmaktadır. Biyometrik özelliklerin kullanıldığı teknolojiler bireyleri birbirlerinden ayırt edebilmek için, sürecin doğası gereği olasılıksal bir yapı sunmaktadır. İçerdiği karmaşıklık, çözüm, teknoloji veya sistem tasarlandığı gibi davranıyor olsa bile, sistem tarafından ölçülen özelliklerin farklılığı ve kararlılığı hakkında zayıf veya eksik bir anlayışın var olabilme ihtimali sebebiyle tüm biyometrik sistemlerde kaçınılmaz bir belirsizlik ve hata riski vardır. "Kullanılan karakteristik ne kadar ayırt edici ise sistem başarısı o kadar iyileşir." düşüncesinden yola çıkılarak, harici karakteristikler ya da mevcut karakteristiklere birlikte kullanılacak ve başarı oranını arttıracaktır. Sosyal ve yumuşak (soft) biyometrik davranışların da sistemleri iyileştirmede kullanılabilecek yardımcı veriler olduğu açıktır.

"Bireyleri nasıl birbirlerinden en iyi şekilde ayırabiliriz?" düşüncesiyle üretilen her bir çözüm, bireylerden daha fazla fiziksel, davranışsal ve kişilik özelliği toplama ile sonuçlanmıştır. Hatta incelenen çalışmalarda da görüldüğü

üzere klasik biyometrik karakteristikler kullanılmadan bile bir grup içinde bireyi ayırt edebilmek mümkün hâle gelmiştir. Bireyler kendilerini teknoloji sayesinde sürekli değişen bir dünyaya alıştırmak zorunda hissetmeleri sebebiyle, sanal dünyada kullandıkları birçok uygulama ile davranışsal ve fiziksel biyometrik verileri paylaşacak birçok eylem gerçekleştirmektedirler. Bu paylaşımların sonucu oluşan veri kümelerinin günümüz teknolojileri ile analiz edilmesinden elde edilen en çarpıcı sonuç, fiziksel dünyada dış görünüşü ve davranışları ile diğerlerinden ayrılan bireyin sanal dünyada bıraktığı ayak izleri ile de aynı şekilde diğerlerinden kolayca ayrılabilmesidir.

Yıllar geçtikçe sayısız nedenden ötürü dünya çapında biyometrik çözümlerin, uygulamaların ve teknolojilerin istikrarlı bir şekilde arttığı görülmektedir. Sınır ve göç kontrolünden suçluları tanımlamaya, iş gücü yönetiminde zaman ve katılımı kontrol etmekten güvenli mekânlar ve şehirlerde yaşayabilme ve güvenli sağlık hizmeti alabilmeye kadar birçok alanda biyometri pratik bir çözüm olarak düşünüldüğünden kullanımı hızla artmaktadır. Yüksek güvenirlikli platformlar üretmek ve hizmet kolaylığı sunabilmek için kullanılan biyometrik verilere farklı bir bakış açısıyla bakıldığında görülmektedir ki; sağlanan her üstünlük, beraberinde paylaşılması zorunlu kılınan bir veri olarak geri dönmektedir. Başka bir deyişle biyometri tabanlı tüm teknolojilerin kullanılmasında en çok endişe edilen nokta, kişisel verilerin kolayca ve rıza olmadan toplanabilmesidir.

Bu bölümde incelenen çalışmalar, bireylerin davranışlarının ve tercihlerinin, psikolojik yapıların altında yatan kişilik özellikleri ile büyük ölçüde açıklanabileceğini göstermiştir. Bireyin kişiliği hakkında bilgi, bağlamlar ve ortamlar arasındaki tercihler, birey hakkında tahminlerde bulunmasına hatta bir grup içinde bireyin teşhis edilmesine olanak sağlar. Bireye ait bu tarz verilerin toplanabileceği en uygun alan olan siber dünya, veri bilimciler için hazine olarak görülmektedir. Çünkü siber dünyayı oluşturan sosyal medya platformları, web siteleri, bloglar vb. kişiselleştirilmiş hizmetler, kullanıcı davranışının çeşitli yönlerini yakalamak için eşsiz birer fırsat sunar. Siber dünya hizmetleri aracılığı ile üretilen verileri anlamlandırabilmek için özellikle büyük veri ve yapay zekâ teknolojilerine artan bir ilgi olduğu görülmektedir. Bu ilginin temel sebebi, bireylerin siber dünyalarında, gerçek dünyalarında bile olmadıkları kadar fazla veriyi rahatlıkla paylaşabilmesi ve bunu yaparken herhangi bir risk görmemesidir.

Yapılan literatür incelemesi ve deneyimlerimiz sonucunda:

- Fizyolojik biyometrinin tek başına kullanılmasının gürbüz bir sistem için ancak kısmi olarak yeterli olduğu, sistemlerin daha güvenli bir hâle getirilmesi, esnek olarak tasarlanması, kolay kullanılması ve daha bütünleşik çözümler için fizyolojik biyometrik özelliklerle birlikte davranışsal biyometrik özelliklerin de kullanılmasıyla yeni, farklı ve esnek ve yüksek performanslı sistemler geliştirilebilecektir.
- Karakter analizi ve davranışsal biyometri arasındaki ilişkiye dayanarak, fiziksel ile birlikte davranışsal ve sosyal biyometrik özelliklerinde kullanılmasıyla tam anlamıyla bir birey tanımlanmasının yanında toplumların da tanımlanmasının mümkün olabileceği net olarak görülmektedir. Bireylerin ve grupların sosyal platformlarda belirli davranış kalıpları oluşturduğu, bu kalıplardan davranışsal ve karakteristiksel özelliklerinin tespit edilebileceği, sosyal biyometri, siber etnografi, veri bilimi ve büyük veri analitiği gibi bilim disiplinlerinden faydalanılarak, adli bilişim, kriminoloji, davranış ve algı bilimi, toplum psikolojisi, bilgisayar bilimleri gibi farklı perspektiflerden bakılarak bireylerin, grupların, toplumların veya ulusların gruplandırılabileceği, sınıflandırılabileceği veya davranışlarının anlamlandırılabileceği değerlendirilmektedir.
- Davranışsal biyometrinin kapsamının daha iyi anlaşılması için verilen örnekler ve özellikler sadece kimlik doğrulama için değil; bunun ötesinde pek çok uygulamanın geliştirilmesi, farklı çözümlerin bulunması, özellikle de vücut dinamikleri ve hareketleri, taşınabilir akıllı cihaz etkileşimleri, yürüyüş, hareket ve estetik biyometrisi, davranış dinamikleri gibi incelenen yöntemlerden elde edilen öznitelikler ile farklı bakış açıları kazanılabilecektir. Sosyal davranışsal biyometrik verilerin analizinin olumlu yansımaları ve toplumun gelişmesine ve korunmasına yönelik olarak yeni çıkarımların elde edilmesine katkı sağlayacağı değerlendirilse de, bu konunun beraberinde bilinen, görünen veya görünmeyen pek çok riski, tehdidi ve tehlikeyi de barındırdığı ortadadır.
- Bu bölümde tanıtılan her türlü yumuşak biyometri ve sosyal davranışsal biyometrisi verilerinin günümüzde sadece kişisel güvenliği değil toplumsal ve ulusal güvenliği de tehdit ettiğinin de mutlaka farkında olunmalıdır. Bu verilere sahip olan şirketler veya ülkeler her zaman-

kinden daha fazla toplanan biyometrik verileri güvenli bir şekilde saklamak, işlemek ve korumak zorundadır. Üçüncü tarafların ilgisini çeken cazibeye sahip olan kullanıcı profil verilerinden çok faydalı çıkarımlar yapılabileceği görülmekte olsa da sahip olunan verilerin kötü niyetli olarak kullanılması durumunda ise ayrımcılığa, istismara veya haksızlığa sebebiyet verebileceği de her zaman hatırda tutulmalıdır.

- Bir kişinin tanımlanmasının tuş vuruş bilgilerinden, yürüyüşünden, konuşmasından, yapılan seçimlerden veya beğenilerden, elektronik ortamlarda bırakılan ayak izlerinden tespit edilebileceği açıktır. Elektronik ortamlardan bir kişiye ait 50.000'in üzerinde farklı parametrenin toplandığı günümüzde, kişileri tanımlamak için bu özelliklerin bir araya getirilerek tespit edilebildiği çalışmalara bakıldığında, özellikle sosyal biyometri kullanılarak bundan sonraki süreçte sadece kişileri tanımlama değil toplumları ve toplulukları gruplandırma ve tanımlamaya üzerine odaklanıldığı düşünüldüğünde, kişileri ve toplumları sınıflandırma, gruplandırma ve ayrıştırma gibi olumsuz yaklaşımlarla karşılaşılabileceği, bu gibi yaklaşımlar ile geleceği tayin etme gücü ve hakkının bu teknolojilere ve verilere sahip toplumların ve ülkelerin elinde olacağı açıktır.
- Teknolojinin gelişmesi kişilerin mahrem bilgilerini kaybetme riskini daha da arttırmaktadır. Davranışsal biyometrik verilerin, fizyolojik verilere göre elde edilebilmesinin daha hızlı ve bazı durumlarda kişinin bilgisi olmadan da toplanabilmesinin de kolay olması sebebiyle, bireylerin rızası ya da bilgisi olmadan gizlice alınıp, işlenme ve yorumlanabilme tehlikesiyle karşı karşıya kalınmaktadır. Bu durum etik kaygıları da beraberinde getirmektedir. Davranışsal biyometrik verilerin toplanıp, işlenmesi ve yorumlanması sonucunda bireyler hakkında gerekenden daha fazla bilgi açığa çıkarılabilir. Bu riskin önlenmesi için davranışsal biyometrik verilerin korunması ve kullanımı konusunda ilgili yasalar çerçevesinde gizliliğin ihlal edilmemesi konusunda daha çok çalışma yapılmalıdır. Her ne kadar kişisel veriler KVKK kapsamında korunuyor görünse de, kişilerin dikkatsizliği, kişisel verilerini dikkatsizce paylaşması veya bunu paylaşabilecek cazip uygulamaların kullanıcılara sunulmasıyla bu sorun varlığını sürdürmeye devam edecektir. 6698 sayılı KVKK gereği özel niteliklere sahip olan biyometrik veriler koruma altındadır. Bu verilerin hangi

şartlarda analiz edilebileceği ilgili Kanun'da çok net olarak ifade edilmiştir. GDPR'da her ne kadar "profil çıkarma" başlığı altında bu konu detaylı olarak ele alınmış olsa da böyle bir veri işleme faaliyetine dayalı bir kararın kullanıcının tercihine bırakıldığı görülmektedir.

- ABD'de 1 Ocak 2020'de yürürlüğe giren CCPA'de (Kaliforniya Tüketici Gizlilik Kanunu), yumuşak (soft) ve sosyal davranış biyometrik verilerinin tanımladığı ve yapılan tanımda "*... kişisel kimlik oluşturmak için fizyolojik, biyolojik veya davranışsal özelliklerinin bir kişinin tek başına, birbirleriyle veya diğer tanımlayıcı verilerle eşleştirilmesi, birleştirilmesi ve kullanılması hâlinde ...*" olarak ifade edildiği görülmektedir. Bu bölümde de üzerinde durulduğu gibi artık tam veya yakın biyometrik özelliklerin bir tehlike oluşturduğu açıktır. Kanunda da açıkça ifade edildiği gibi 50.000'den fazla kullanıcının verisini toplayan, 25 milyon dolar ve üzeri bütçesi olan, gelirinin yarısından fazlasını müşterilerin kişisel verilerini satarak kazanç elde eden şirketlerin belirtilen kanunda artık uymak zorunda oldukları hususlar net olarak ifade edilmiştir. Şirketlerin; kişisel verileri korumak ve ihlalleri önlemek zorunda oldukları, kullanıcıların istemeleri durumunda bu şirketlerin kişisel veriler ile ilgili olarak kullanıcıyı bilgilendirmek, verileri silmek zorunda oldukları, buna ilave olarak ta karşılaşılan her hangi bir olumsuz durum veya olay durumunda, olay başına kişilerin 100-750 dolar, şirketlerin ise 7500 dolara kadar cezaya çarptırılabilecekleri belirtilmektedir. Bu kanunun ABD'de ilk olması sebebiyle de büyük şirketlerin sadece biyometrik veri değil diğer kişisel verileri korumada da daha dikkatli olacakları açıktır.
- Gelecek çalışmalarda, adli bilişim bakış açısıyla ve bilgisayar bilimleri çözümüyle, bir bireyi/toplumu tanımlamak için kullanılan fiziksel ve davranışsal biyometrik karakteristiklerin dışında, tek başına anlam ifade etmeyen ama birlikte değerlendirildiğinde veya analiz edildiğinde bireyi/toplumu/ulusu ayırt edebilecek kapasiteye sahip belirli özellikler kullanılarak bir bireyin sosyal biyometrik kimlik belirlenmesi, toplumların davranış modellerinin çıkartılması ve siber etnografik analizinin yapılması ötesinde ulusların da analiz edilebileceği de her zaman dikkate alınmalıdır.
- Her ne kadar burada sosyal davranış biyometrisine yönelik olarak çalışmalar yapıldığı belirtilse de, büyük boyutta olan verilere sahip

olmak, bu verileri kapsamlı analiz etmek, farklı ve büyük çıkarımlar yapmak, kişisel veya kurumsal çıkarımların ötesinde ulusal boyutta çıkarımlar elde etmek ise işin diğer belki de en önemli boyutudur. Bu konunun kişisel güvenlikten ulusal güvenlik boyutuna kadar pek çok aşamada değerlendirilmesi gereklidir. Bu konu kişisel veri güvenliğinden öte ulusal bir konu olup üzerinde daha çok konuşulması, tartışılması ve yeni çözüm ve bakış açılarının geliştirilmesi gereken bir konudur.

- Biyometrik verilerin çoğunlukla erişim kontrolü için tercih edildiği bir gerçektir. Bunun yanında bu veriler, delilden suçluya gitmede ve suçluların tespitinde önemli bir rol oynar. Bu açıdan bakıldığında, sanal ortamlarda kişilerin mahremiyetinin kolaylıkla ihlal edilebileceği bir gerçek ise de, bu ortamlarda suç işleyenlerin belirlenmesi, tespiti ve delillendirilmesi de mümkün olabilecektir. Bu konuya da özellikle önem vermeli, federe öğrenme gibi güncel çözümler geliştirilmeli ve kullanılmalıdır.
- Sağıroğlu ve ekibi [66] tarafından önerilen bir biyometrik özellikten diğer bir biyometrik özelliğin çıkarılabileceğine dair yapılan çalışmalar dikkate alındığında, gelecekte bu konunun daha da önemli hâle geleceği ortadadır. Özellikle, MIT'de yapılan son çalışmalarda sesten yüz eşkalinin çıkarılabileceğine dair yapılan çalışmalardan elde edilen başarılarda bunun diğer bir önemli göstergesidir.
- Biyometrik veriler ister nitelikli isterse yumuşak veya sosyal davranışsal biyometrik veriler olsun hatırda her zaman tutulması gereken veya unutulmaması gereken en önemli husus, biyometrik verilerin değişmez olması sebebiyle, bir kez ele geçirildiğinde kullanıcının ömür boyu bu özelliklerinin risk altında olabileceği unutulmamalı ve gerekli önlemler alınmalıdır.

Bu bölümde bireyi tek başına tanımlamaya yetecek biyometrik özelliklerin ötesinde tüm biyometrik özellikler kullanıldığında en az biyometrik bir karakteristik kadar bireye has olduğu düşünülen yarı biyometrik özellik ve karakteristiklerin nasıl ve ne şekilde elde edildiği, bu özelliklerin hangi amaçlarla ve nasıl kullanılabileceği, elde edilecek büyük kazanımların yanı sıra içerisinde de büyük riskleri barındırmakta olduğu aşikârdır. Bireylerin, toplumların veya ülkelerin ürettikleri, istedikleri, paylaştıkları, yaptıkları ile aldıkları önlemler burada belirleyici olacaktır.

KAYNAKLAR

[1] Buciu, I. ve Gacsadi, A. (2016). Biometrics systems and technologies: a survey. International Journal of Computers Communications & Control, 11(3), 315-330.

[2] Jain, A. K., Nandakumar, K. ve Ross, A. (2016). 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern recognition letters*, *79*, 80-105.

[3] Bhatt, S. ve Santhanam, T. (2013). Keystroke dynamics for biometric authentication—A survey. In *2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering*, 17-23.

[4] Ashbaugh, D. R. (1999). Quantitative-qualitative friction ridge analysis: an introduction to basic and advanced ridgeology, CRC press.

[5] The History of Fingerprints. URL: http://www.onin.com/fp/fphistory.html, Son Erişim Tarihi: 30.11.2020.

[6] Barnes, J. G. (2010). Fingerprint sourcebook-chapter 1: History.

[7] National Research Council ve Whither Biometrics Committee. (2010). Biometric recognition: challenges and opportunities National Academies Press.

[8] Biometrics History - Homeland Security Digital Library. URL: https://www.hsdl.org/, Son Erişim Tarihi: 01.12.2020.

[9] Jain, A. K., Ross, A. ve Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology*, *14* (1), 4-20.

[10] Preece, J., Sharp, H., Rogers, Y. (2015). Interaction design: beyond human-computer interaction. John Wiley & Sons.

[11] Blanco-Gonzalo, R., Miguel-Hurtado, O., Lunerti, C., Guest, R. M., Corsetti, B., Ellavarason, E. ve Sanchez-Reillo, R. (2019). Biometric Systems Interaction Assessment: The State of the Art. *IEEE Transactions on Human-Machine Systems*, *49* (5), 397-410.

[12] Yampolskiy, R. V. ve Govindaraju, V. (2008). Behavioural biometrics: a survey and classification. International Journal of Biometrics, 1 (1), 81-113.

[13] Schuett, M. (2018). "Rationalizing Behavioral Biometrics", ISSA Developing and Connecting Cybersecurity Leaders Globally.

[14] Singh, J. P., Jain, S., Arora, S. ve Singh, U. P. (2018). Vision-based gait recognition: A survey. *IEEE Access*, *6*, 70497-70527.

[15] Little, J. ve Boyd, J. (1998). Recognizing people by their gait: the shape of motion. *Videre: Journal of computer vision research*, *1* (2), 1-32.

[16] Li, Z. ve Yuan, P. (2017). Research on gait recognition algorithm based on contour feature fusion. In *2017 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*, 1-5.

[17] Sun, Y. ve Lo, B. (2018). An artificial neural network framework for gait-based biometrics. *IEEE journal of biomedical and health informatics*, *23* (3), 987-998.

[18] Young, J. R. ve Hammon, R. W. (1989). *U.S. Patent No. 4,805,222*. Washington, DC: U.S. Patent and Trademark Office.

[19] Alves, D. D., Cruz, G. ve Vinhal, C. (2014, December). Authentication system using behavioral biometrics through keystroke dynamics. In 2014 IEEE Symposium on Computational Intelligence in Biometrics and Identity Management (CIBIM), 181-184.

[20] Tsimperidis, I., Yoo, P. D., Taha, K., Mylonas, A. ve Katos, V. (2018). R 2 BN: An Adaptive Model for Keystroke-Dynamics-Based Educational Level Classification. IEEE transactions on cybernetics, 50 (2), 525-535.

[21] Cai, Z., Shen, C. ve Guan, X. (2014). Mitigating behavioral variability for mouse dynamics: A dimensionality-reduction-based approach. *IEEE Transactions on Human-Machine Systems*, *44* (2), 244-255.

[22] Ahmed, A. A. E. ve Traore, I. (2007). A new biometric technology based on mouse dynamics. IEEE Transactions on dependable and secure computing, 4 (3), 165-179.

[23] Shen, C., Cai, Z., Guan, X., Du, Y. ve Maxion, R. A. (2012). User authentication through mouse dynamics. *IEEE Transactions on Information Forensics and Security*, *8* (1), 16-30.

[24] Jayamaha, R. M. M., Senadheera, M. R., Gamage, T. N. C., Weerasekara, K. P. B., Dissanayaka, G. A. ve Kodagoda, G. N. (2008). Voizlock-human voice authentication system using hidden markov model. In *2008 4th International Conference on Information and Automation for Sustainability*, 330-335.

[25] Mason, J. S. ve Brand, J. D. (2002). The role of dynamics in visual speech biometrics. In *2002 IEEE International Conference on Acoustics, Speech, and Signal Processing,* IV-4076-IV-4079.

[26] Mahesh, P. K. ve Swamy, M. S. (2010). A biometric identification system based on the fusion of palmprint and speech signal. In *2010 International Conference on Signal and Image Processing*, 186-190.

[27] Kaur, G., Singh, D. ve Kaur, S. (2014). Pollination based optimization for feature reduction at feature level fusion of speech & signature biometrics. In *Proceedings of 3rd International Conference on Reliability, Infocom Technologies and Optimization*, 1-6.

[28] Lovato, P., Bicego, M., Segalin, C., Perina, A., Sebe, N. ve Cristani, M. (2014). Faved! biometrics: Tell me which image you like and I'll tell you who you are. *IEEE Transactions on Information Forensics and Security*, *9* (3), 364-374.

[29] Azam, S. ve Gavrilova, M. (2016). Soft biometric: give me your favorite images and I will tell your gender. In *2016 IEEE 15th International Conference on Cognitive Informatics & Cognitive Computing (ICCI* CC)*, 535-541.

[30] Sieu, B. ve Gavrilova, M. (2019). Person Identification from Visual Aesthetics Using Gene Expression Programming. In *2019 International Conference on Cyberworlds (CW),* 279-286.

[31] Stolfo, S., Hu, C. W., Li, W. J., Hershkop, S., Wang, K. ve Nimeskern, O. (2003). Combining behavior models to secure email systems.

[32] Yampolskiy, R. V. ve Govindaraju, V. (2007). Direct and indirect human computer interaction based biometrics. *JCP*, *2* (10), 76-88.

[33] Zargarzadeh, M. ve Maghooli, K. (2013). A behavioral biometric authentication system based on memory game. *Biosci. Biotechnol. Res. Asia*, *10* (2), 781-787.

[34] Al-Khazzar, A. ve Savage, N. (2010). Behavioural Authentication Using Computer Games. *PgNET*, *2010*, 139-43.

[35] Kore, S. ve Apte, S. (2012). The current state of art: handwriting a behavioral biometric for person identification and verification. In *Proceedings of the International Conference on Advances in Computing, Communications and Informatics*, 925-930.

[36] Tian, J., Qu, C., Xu, W. ve Wang, S. (2013). KinWrite: Handwriting-Based Authentication Using Kinect. In *NDSS*, 93, 94.

[37] Jiang, W., Xiang, J., Liu, L., Zha, D. ve Wang, L. (2013). From mini house game to hobby-driven behavioral biometrics-based password. In *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, 712-719.

[38] Rigas, I., Economou, G. ve Fotopoulos, S. (2012). Biometric identification based on the eye movements and graph matching techniques. *Pattern Recognition Letters*, *33* (6), 786-792.

[39] Juhola, M., Zhang, Y. ve Rasku, J. (2013). Biometric verification of a subject through eye movements. *Computers in biology and medicine*, *43* (1), 42-50.

[40] Alzubaidi, A. ve Kalita, J. (2016). Authentication of smartphone users using behavioral biometrics. *IEEE Communications Surveys & Tutorials*, *18*(3), 1998-2026.

[41] Robertson, J. ve Guest, R. (2015). A feature based comparison of pen and swipe based signature characteristics. *Human movement science*, *43*, 169-182.

[42] Peng, G., Zhou, G., Nguyen, D. T., Qi, X., Yang, Q. ve Wang, S. (2016). Continuous authentication with touch behavioral biometrics and voice on wearable glasses. *IEEE transactions on human-machine systems*, *47* (3), 404-416.

[43] Bevan, C. ve Fraser, D. S. (2016). Different strokes for different folks? Revealing the physical characteristics of smartphone users from their swipe gestures. *International Journal of Human-Computer Studies*, *88*, 51-61.

[44] Zhou, L., Kang, Y., Zhang, D. ve Lai, J. (2016). Harmonized authentication based on ThumbStroke dynamics on touch screen mobile phones. *Decision Support Systems*, *92*, 14-24.

[45] Kambourakis, G., Damopoulos, D., Papamartzivanos, D. ve Pavlidakis, E., (2014). "Introducing touchstroke: keystroke-based authentication system for smartphones", Security and Communication Networks, 9 (6): 542–554.

[46] Sae-Bae, N., Memon, N., Isbister, K. ve Ahmed, K., (2014). "Multitouch gesture-based authentication", IEEE transactions on information forensics and security, 9 (4), 568-582.

[47] Frank, M., Biedert, R., Ma, E., Martinovic, I. ve Song, D. (2012). Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE transactions on information forensics and security*, *8* (1), 136-148.

[48] Akıllı cihaz profilleri, URL: https://finance.arvato.com/496ece/globalassets/03-info graphics/01-corp/01-solutions/01-id-and-fraud-management/fraud-user-profile.jpg, Son Erişim Tarihi: 01.12.2020.

[49] Statista. "Social media - Statistics & Facts". URL: https://www.statista.com/topics/1164 /social-networks/#dossierSummary__chapter5, Son Erişim Tarihi: 01.12.2020.

[50] Statista. "Worldwide digital population as of October 2020 (in millions)". URL: https://www.statista.com/statistics/617136/digital-population-worldwide/, Son Erişim Tarihi: 01.12.2020.

[51] Mordini E. (2013). Biometrics. In Henk A. M. J. ten Have, Bert Gordijn (eds) Handbook of Global Bioethics Berlin: Springer, 341–356.

[52] Mordini, E. ve Ashton, H. (2012). The transparent body: medical information, physical privacy and respect for body integrity. In Second generation biometrics: the ethical, legal and social context, (257-283). Springer.

[53] Bertillon, A. ve McClaughry, R. W. (1896). Signaletic instructions including the theory and practice of anthropometrical identification. Werner Company.

[54] Frank, M., Biedert, R., Ma, E., Martinovic, I. ve Song, D. (2012). Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE transactions on information forensics and security*, *8* (1), 136-148.

[55] Yang, S. J., Greenberg, A. M. ve Endsley, M. (2012). Social computing, behavioral-cultural modeling and prediction. College Park, MD: Springer, 238.

[56] Sultana, M., Paul, P. P. ve Gavrilova, M. (2014). Mining social behavioral biometrics in Twitter. In *2014 International Conference on Cyberworlds*, pp. 293-299.

[57] Sultana, M., Paul, P. P. ve Gavrilova, M. L. (2017). User recognition from social behavior in computer-mediated social context. *IEEE Transactions on Human-Machine Systems*, *47* (3), 356-367.

[58] Sultana, M. ve Gavrilova, M. (2018, October). Temporal Pattern in Tweeting Behavior for Persons' Identity Verification. In *2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 2472-2477.

[59] Delgado-Gómez, D., Sukno, F., Aguado, D., Santacruz, C. ve Artés-Rodriguez, A. (2010). Individual identification using personality traits. *Journal of network and computer applications*, *33* (3), 293-299.

[60] Golbeck, J., Robles, C., Edmondson, M. ve Turner, K. (2011). Predicting personality from twitter. In *2011 IEEE third international conference on privacy, security, risk and trust and 2011 IEEE third international conference on social computing*,149-156.

[61] Golbeck, J., Robles, C. ve Turner, K. (2011). Predicting personality with social media. In *CHI'11 extended abstracts on human factors in computing systems*, 253-262.

[62] Adali, S. ve Golbeck, J. (2012, August). Predicting personality with social behavior. In *2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, 302-309.

[63] Kalghatgi, M. P., Ramannavar, M. ve Sidnal, N. S. (2015). A neural network approach to personality prediction based on the big-five model. *International Journal of Innovative Research in Advanced Engineering (IJIRAE)*, *2* (8), 56-63.

[64] Gu, H., Wang, J., Wang, Z., Zhuang, B. ve Su, F. (2018). Modeling of user portrait through social media. In *2018 IEEE International Conference on Multimedia and Expo (ICME)*, 1-6.

[65] Lien, C. Y., Bai, G. J. ve Chen, H. H. (2019). Visited Websites May Reveal Users' Demographic Information and Personality. In *2019 IEEE/WIC/ACM International Conference on Web Intelligence (WI)*, 248-252.

[66] Ozkaya N. ve Sagiroglu S., Generating One Biometric Feature from Another: Faces from Fingerprints, Sensors, cilt. 10, ss. 4206-4237, 2010.

Bölüm 7

KAFES TABANLI KRİPTOGRAFİDE KULLANILAN ZOR PROBLEMLERİN KRİPTANALİZİ VE YAZILIM KÜTÜPHANELERİ

Hami Satılmış - Sedat Akleylek

Bu bölümde, kuantum sonrası döneme ait olan kafes tabanlı kriptosistem ailesinde bulunan eleme, numaralandırma ve indirgeme kriptanaliz algoritmalarından, bu algoritmaların uygulamalarından ve uygulamaların altyapı olarak kullandıkları yazılım kütüphanelerinden bahsedilmiştir. Literatürde bulunan eleme algoritmalarından GaussSieve, ProGaussSieve, HashSieve, ENUM numaralandırma ve BKZ indirgeme algoritmalarının çalışma düzenleri anlatılmıştır ve eleme algoritmalarının özellikleri karşılaştırılmıştır. Bu algoritmalara ait uygulamaların ve bu uygulamaların altyapı olarak kullandıkları kütüphanelerin özellikleri ifade edilmiştir ve yazılım kütüphaneleri karşılaştırılmıştır.

7.1. GİRİŞ

Shor tarafından geliştirilen ve polinom zamanda çalışan algoritmanın [1] kuantum bilgisayarlar üzerinde uygulanmasıyla, günümüzde kullanılmakta olan RSA, DSA ve ECDSA gibi kriptosistemlerde güvenlik açığının oluşacağı görülmüştür [2]. Daha açık bir ifadeyle, güvenlikleri çarpanlara ayırma ve ayrık logaritma gibi zor problemlerden oluşmakta olan bu günümüz mevcut kriptosistemlerinin, kuantum bilgisayarların kullanılmasıyla polinom zamanda çözülebilecekleri öngörülmektedir [2]. Bu nedenden dolayı, kuantum bilgi-

sayarların günlük hayatta yaygınlaşmasından sonra güvenlik açığının ortaya çıkmaması için yeni kriptosistem ailelerine ihtiyaç duyulmaktadır. Bu kriptosistem ailelerinden olan kafes tabanlı kriptosistemler, günümüz kriptosistemler ile benzer anahtar boyutlarına sahip olmalarından ve performans olarak benzer özellikler göstermelerinden dolayı, oldukça ilgi gören çalışma alanı hâline gelmişlerdir [3]. En kötü zorluğa dayanmakta olan, güvenli sayılan uygulamalardan ve güvenlik ispatlarından yararlanmakta olan kafes tabanlı kriptosistemlerin güvenliği, en kısa vektör problemi (shortest vector problem - SVP) ve en yakın vektör problemi (closest vector problem - CVP) gibi zor problemlere dayanmaktadır [4,5]. Kuantum bilgisayarların kullanılmasıyla bile çözümü çok zor olan bu problemlerin çözülmesi demek, kafes tabanlı kriptosistemlerin güvenliğini azaltmak veya yok etmek anlamına gelmektedir.

SVP ve CVP gibi problemlerin çözümü için literatürde, eleme (sieving) tabanlı, numaralandırma (enumeration) tabanlı ve indirgeme (reduction) algoritmaları olmak üzere, birçok kriptanaliz algoritma aileleri önerilmiştir [6,7,8]. Kafes tabanlı kriptosistemlerin kullandıkları parametrelerin güvenliğini test etmek için kullanılmakta olan bu algoritmalar, hangi parametrelerin daha güvenli olduğuna dair bir bakış açısı sunmaktadır. Başka bir ifadeyle, bu algoritmalar güvenli parametre seçiminde kullanılmaktadır ve bu güvenli parametreleri kullanan kafes tabanlı kriptosistemler, saldırılara karşı daha dirençli olmaktadır.

Güvenli parametre seçilmesinde oldukça önemli bir role sahip olan algoritmalara ait birçok uygulama bulunmaktadır [6,7,8,9,10]. Bu uygulamaların birçoğu, literatürde bulunan yazılım kütüphaneleri [11,12,13,14] altyapı olacak şekilde kullanılarak geliştirilmiştir ve bu uygulamaların bazıları altyapı olarak kullandıkları yazılım kütüphanelerine eklenmiştir.

Bu bölümün ikinci başlığı altında, literatürdeki eleme tabanlı ve numaralandırma tabanlı algoritmalardan, uygulamalardan ve yazılım kütüphanelerinden bahsedilmektedir. Üçüncü başlık altında, GaussSieve, ProGaussSieve, HashSieve eleme algoritmalarının, ENUM numaralandırma algoritmasının ve BKZ indirgeme algoritmasının çalışma düzenleri sözde kodlar üzerinden anlatılmaktadır ve eleme algoritmaları karşılaştırılmaktadır. Dördüncü başlık altında, bu kriptanaliz algoritmalarına ait literatürdeki uygulamaların ve bu uygulamalar geliştirilirken kullanılan veya bu uygulamaları içermekte olan yazılım kütüphanelerinin üzerinde durulmaktadır. Son olarak beşinci başlıkta ise, bu bölümde anlatılan konular ile ilgili elde edilen sonuçlar kısaca ifade edilmektedir.

7.2. LİTERATÜR ÖZETİ

Bu başlık altında, literatürde SVP problemini çözmek için önerilen, eleme tabanlı algoritmalardan, numaralandırma tabanlı algoritmalardan, indirgeme algoritmalarından ve bu algoritmaların uygulamalarından bahsedilmektedir. Ayrıca, bu uygulamaları geliştirirken kullanılan ve bazı uygulamaları içerisinde barındırmakta olan yazılım kütüphanelerine değinilmektedir.

7.2.1. Eleme Algoritmaları ve Uygulamaları

SVP'ni çözmek ve kafes tabanlı kriptosistemlerde güvenli parametre seçmek için kullanılan eleme algoritmalarının altında yatan ana ortak düşünce, işleme boş bir liste veri yapısıyla başlamak ve liste en kısa vektörü içerene kadar her bir iterasyonda listeye daha kısa vektör eklemektir [15]. Literatürde, GaussSieve [6] ve ProGaussSieve [7] gibi birbiri ile doğrudan bağlantılı ve biri diğerini temel alarak geliştirilen birçok eleme algoritması önerilmiştir. Eleme algoritmalarının bilinen ilk üstel zamanlı algoritması olan AKS (Ajtai-Kumar-Sivakumar) algoritması, 2001 yılında Ajtai tarafından ortaya çıkarılmıştır ve n kafes boyutu olacak şekilde, $2^{2.465n+o(n)}$ asimptotik çalışma zamanı ve $2^{1.233n+o(n)}$ alan karmaşıklığında çalışmaktadır [16]. Nguyen ve Vidick tarafından geliştirilen ve AKS eleme algoritmasının sezgisel versiyonu olan algoritma ile, AKS algoritmasını pratiğe dönüştürülebilmenin mümkün olduğu fakat kafes büyüdükçe bellek problemi oluşacağı sonucuna varılmaktadır [17]. $2^{3.199n+o(n)}$ asimptotik çalışma zamanı ve $2^{1.325n+o(n)}$ alan karmaşıklığı değerlerine sahip olan ListSieve eleme algoritması, boş bir liste veri yapısı ile eleme işlemine başlamaktadır ve en kısa vektörü bu listeye ekleyene kadar, elde ettiği kısa kafes vektörlerini bu listede tutmaktadır [6]. 2010 yılında, ListSieve algoritmasını da geliştiren Micciancio ve Voulgaris tarafından tasarlanan GaussSieve eleme algoritması, ListSieve algoritması ile aralarında bir kaç yapısal farklılık olsa da, ListSieve ile aynı ana mantık altında çalışmaktadır [6]. GaussSieve algoritması, $2^{0.48n+o(n)}$ asimptotik çalışma zamanı ve $2^{0.18n+o(n)}$ alan karmaşıklığında işlem yapmaktadır [6]. Bir başka Gauss tabanlı eleme algoritması olan ve GaussSieve algoritmasının kademeli versiyonu olan ProGaussSieve (Progressive GaussSieve - Kademeli GaussSieve) algoritması ortaya çıkartılmıştır [7]. Laarhoven ve Mariano tarafından 2018 yılında ortaya çıkartılan ProGaussSieve eleme algoritması, asimptotik olarak $2^{0.42n+o(n)}$ çalışma zamanı ve $2^{0.21n+o(n)}$ alan karmaşıklığı değerlerinde çalış-

maktadır [7]. Laarhoven, Charikar'ın bölgesel duyarlı kıyım (locality sensitive hash - LSH) yöntemini GaussSieve algoritmasına uygulayarak, HashSieve eleme algoritmasını geliştirmiştir [8]. Asimptotik $2^{0.3366n+o(n)}$ çalışma zamanı ve alan karmaşıklık değerlerinde [8] işlem yapmakta olan HashSieve algoritması, GaussSieve algoritmasından daha hızlı bir şekilde çalışmaktadır [18].

Bu eleme algoritmalarından bazıları, standart veya paralel yapılı olmak üzere pratik olarak gerçekleştirilmiştir. Micciancio ve Voulgaris, NTL [12] yazılım kütüphanesini altyapı olarak kullanarak, GaussSieve algoritmasına ait standart uygulamayı geliştirmişlerdir [6]. GaussSieve algoritmasının bir diğer standart uygulaması, Satılmış ve Akleylek tarafından, kendi geliştirdikleri modüler yapılı yazılım kütüphanesi altyapı olarak kullanılarak gerçeklenmiştir [10]. Paralel programlama yöntemi ile pratiğe dökülen ilk paralel yapılı GaussSieve uygulaması, Milde ve Schneider tarafından geliştirilmiştir [19]. Ishiguro ve arkadaşları, CPU üzerinde dağıtık bellek yöntemini kullanarak, GaussSieve algoritmasına ait bir başka paralel yapılı uygulamayı ortaya çıkarmışlardır [20]. GaussSieve algoritmasının bir başka paralel yapılı uygulaması, Mariano ve arkadaşları tarafından, kilitsiz bağlantılı liste (lock-free list) veri yapısı kullanılarak geliştirilmiştir [21]. 2017 yılında, bilinen ilk GPU üzerinde pratiğe dökülen paralel yapılı GaussSieve algoritmasına ait olan uygulama, Yang ve arkadaşları tarafından gerçeklenmiştir [22]. Bir başka Gauss tabanlı eleme algoritması olan ProGaussSieve algoritmasına ait uygulama, algoritmayı ortaya çıkartan Laarhoven ve Mariano tarafından geliştirilmiştir [7]. Satılmış ve Akleylek, ProGaussSieve algoritmasının standart bir uygulamasını, kendilerinin geliştirdikleri yazılım kütüphanesini kullanarak ortaya çıkarmışlardır [10]. 2015 yılında, Gauss tabanlı eleme algoritmalarından olan HashSieve algoritmasına ait standart uygulama, Laarhoven tarafından geliştirilmiştir [8]. Satılmış ve Akleylek, Laarhoven'in geliştirdiği bu uygulamayı temel alarak, üzerinde bazı yazılımsal değişiklikler yaparak ve kendi yazılım kütüphanelerini altyapı olarak kullanarak, HashSieve algoritmasını pratiğe dökmüşlerdir [14].

7.2.2. Numaralandırma Algoritmaları ve Uygulamaları

Eleme algoritmalarından farklı olarak SVP probleminin çözümü için geliştirilen diğer kriptanaliz algoritmaları ise, numaralandırma tabanlı algoritmalardır. Temel olarak aynı çalışma düzeninde işlem yapmakta olan bu algorit-

maların ana mantığı, sınırlandırılan bir alandaki tüm noktaları veya başka bir deyişle tüm kafes vektörlerini sistematik bir şekilde numaralandırarak en kısa vektörü bulmaktır. Literatürde bilinen ilk numaralandırma tabanlı algoritmaları, Kannan algoritması [23] ile Fincke ve Pohst algoritmasıdır [24]. 1991 yılında Schnorr ve Euchner, numaralandırma algoritmaları arasında en ilgi duyulan ve BKZ indirgeme algoritmasında [9] kullanılmak amacıyla tasarlanan, ENUM numaralandırma algoritmasını ortaya çıkarmışlardır [25]. "Aşırı Budama" yöntemini numaralandırma algoritmalarına uygulayan Gama ve arkadaşları, bu algoritmaların daha verimli çalışmalarını sağlamışlardır [26]. Numaralandırma algoritmaları içerisinde en popüler olanı olan ENUM algoritmasına ait birçok uygulama bulunmaktadır. Bu uygulamaların ilki olarak bilinen uygulama, algoritmayı da geliştiren Schnorr ve Euchner tarafından, BKZ algoritmasının alt işlemi olarak gerçeklenmiştir [9]. Daha sonra Dağdelen ve Schneider, ENUM algoritmasına paralel programlama tekniği uygulayarak, ilk paralel yapılı ENUM uygulamasını geliştirmişlerdir [27]. 2016 yılında, ENUM algoritmasına ait bir başka paralel yapılı uygulama olan SE++, Correia ve arkadaşları tarafından pratiğe dökülmüştür [28].

Kafes tabanlı kriptosistemlerde kullanılmak üzere güvenli parametre seçmeye yardımcı olan ve bu kriptosistemlerde bulunan SVP problemlerini çözmek için geliştirilen eleme ve numaralandırma algoritmaları çalışmaya başlamadan önce, Gram-Schmidt [29], LLL [30] ve BKZ gibi indirgeme algoritmaları, kafeslerin boyutlarını indirgemek amacıyla kullanılmaktadır. İndirgeme algoritmaları içerisinde en verimli çalışan BKZ algoritması, LLL indirgeme algoritmasının farklı versiyonlarını ve numaralandırma algoritmalarını alt işlem olarak kullanmaktadır. LLL indirgeme algoritmasının bloklu hâli [31] olan BKZ algoritması, Schnorr ve Euchner tarafından ortaya çıkarılmıştır ve daha sonra pratiğe dökülmüştür [9]. Chen ve Nguyen, BKZ algoritmasının farklı bir versiyonu olan BKZ 2.0 algoritmasını, erken durdurma [31], kademeli indirgeme ve budamalı numaralandırma yöntemlerini kullanarak ortaya çıkarmışlardır ve algoritmanın uygulamasını geliştirmişlerdir [32]. 2014 yılında Liu ve arkadaşları, BKZ algoritmasının paralel yapılı olan uygulamasını tanıtmışlardır [33]. Correia, farklı bloklar üzerinde paralel olarak işlem yapabilecek şekilde, BKZ algoritmasının bir başka versiyonu olan ACBKZ algoritmasını önermiştir ve bu algoritmanın uygulamasını geliştirmiştir [34].

7.2.3. Kriptanaliz Yazılım Kütüphaneleri

Eleme, numaralandırma ve indirgeme algoritmalarına ait uygulamaların geliştirilmesinde altyapı olarak kullanılabilir yapıda olan ve içlerinde birçok hazır bileşeni barındıran yazılım kütüphaneleri bulunmaktadır. Bu yazılım kütüphaneleri içerisinde en popüler kütüphanelerden birisi olan NTL, C++ programlama dili ile geliştirilmiştir. Açık kaynak kodlu olan NTL kütüphanesi, kriptanaliz algortimalarının işlem yaparken sıklıkla kullandıkları değişik matematiksel işlemleri ve Gram-Schmidt, LLL, Numaralandırma, BKZ gibi algoritmaları hazır fonksiyon olarak içerisinde barındırmaktadır. Oldukça ilgi gören bir başka yazılım kütüphanesi olan fplll kütüphanesi [11], C++ programlama dili ile geliştirilmiştir ve açık kaynak kodlu bir yazılım kütüphanesidir. Kriptanaliz algoritmalarının alt işlem olarak sürekli kullandıkları matematiksel işlemleri ve Gram-Schmidt, LLL, numaralandırma, BKZ, Klein'in En Yakın Komşu [35] gibi algoritmaları kullanılmaya hazır yapılar olarak bulunduran fplll kütüphanesinde, bu hazır yapılar kullanılarak geliştirilen GaussSieve eleme uygulaması da bulunmaktadır. Açık kaynak kodlu olan bir başka önemli yazılım kütüphanesi olan plll kütüphaneside [13] C++ programlama dili ile gerçeklenmiştir. plll kütüphanesi içerisinde, matematiksel işlem yapılarını ve LLL, Numaralandırma, BKZ gibi birçok algoritmayı bulundurmaktadır.

Tablo 7.1. Yazılım kütüphanelerinin içerdikleri uygulamalar ve bileşenler

Yazılım Kütüphanesi	Programlama Dili	Uygulamalar ve Bileşenler
fplll [11]	C++	Gram-Schmidt, LLL, LLLFP, Numaralandırma, BKZ, BKZ 2.0, HKZ, KleinSampler, GaussSieve
NTL [12]	C++	Gram-Schmidt, LLL, BKZ
plll [13]	C++	Gram-Schmidt, LLL, Numaralandırma, BKZ, Voronoi Hücresi, Çeşitli Eleme Algoritmaları
Modüler Yazılım Kütüphanesi [14]	C	Gram-Schmidt, LLL, LLLFP, GaussReduce, ENUM, nearA, randRound

Satılmış ve Akleylek tarafından geliştirilen bir başka yazılım kütüphanesi, modüler yapıda olacak şekilde, kriptanaliz algoritmalarına ait uygulamalarda altyapı olacak şekilde tasarlanmıştır [14]. GaussSieve, ProGaussSieve, HashSieve, ENUM ve BKZ algoritmalarına ait uygulamalar geliştirilirken kullanılan bu modüler yazılım altyapı kütüphanesi, C programlama dili kullanılarak geliştirilmiştir. Satılmış ve Akleylek tarafından geliştirilen bu yazılım kütüphanesi, matematiksel işlemleri ve Gram-Schmidt, LLL, ENUM, GaussReduce [6], Klein'in En Yakın Komşu algoritmalarını birer modül olarak içermektedir. İçerisinde, çeşitli eleme ve numaralandırma algoritmalarının paralel yapılı ve yüksek performanslı uygulamalarını barındırmakta olan LUSA yazılım kütüphanesi, Mariano tarafından geliştirilmiştir [36]. Kafes tabanlı kriptografi alanında en çok ilgi görmekte olan fplll, NTL, plll yazılım kütüphanelerinin ve modüler yazılım kütüphanesinin içerdiği uygulamalar, Tablo 7.1'de gösterilmektedir.

7.3. KRİPTANALİZ ALGORİTMALARI

Bu bölümde, en kısa vektör probleminin çözümü için kullanılmakta olan GaussSieve, ProGaussSieve, HashSieve eleme algoritmalarından, ENUM numaralandırma algoritmasından ve BKZ indirgeme algoritmasından bahsedilmektedir.

7.3.1. Eleme Tabanlı Algoritmalar

SVP probleminin çözümü için geliştirilmiş ve çoğunlukla aynı mantık altında ve çalışma düzeninde işlem yapmak olan eleme algoritmalarından, GaussSieve, ProGaussSieve ve HashSieve algoritmalarına ait özellikler, bu başlık altında anlatılmaktadır. Bu kriptanaliz algoritmalarına ait çalışma düzenleri, sözde kodlar üzerinden anlatılmaktadır. Ayrıca, bu algoritmalara ait karmaşıklık değerlerini, içerdikleri ana mantıklarını ve temel işlemlerini karşılaştıran bir tablo sunulmaktadır (Tablo 7.2).

7.3.1.1. GaussSieve ve ProGaussSieve Eleme Algoritmaları

Micciancio ve Voulgaris tarafından ortaya çıkartılan GaussSieve eleme algoritmasının ana düşüncesi, kafes vektörlerinin bulunduğu liste yapısına her bir

iterasyonda daha kısa olacak şekilde bir kafes vektörü dâhil etmektir. Bu ana düşünceye ek olarak GaussSieve algoritması, kafes vektörlerinin bulunduğu vektörler ile yeni bulduğu kafes vektörünü indirgemektedir (Öklid uzunluğunu küçültmek). Bu işlemden sonra, indirgediği yeni kafes vektörü ile listede bulunan kafes vektörlerini indirgemektedir.

Algoritma 1'de bulunmakta olan sözde kodun mavi ile yazılmış satırları kaldırılınca elde edilen GaussSieve algoritması girdi parametreleri olarak, indirgenmiş B kafesini ve durdurma kriteri c maksimum çakışma sayısını (sıfır vektör sayısı) almaktadır. GaussSieve algoritması bir iterasyonda ilk olarak, örnek vektörleri saklamak için kullandığı S yığın veri yapısından veya Klein'in En Yakın Komşu algoritmasını kullanarak yeni bir v örnek vektörünü işleme sokmaktadır. Bu v yeni örnek vektör, GaussReduce algoritması tarafından tüm w liste vektörleri kullanılarak indirgenmektedir. İndirgenmiş olan v örnek vektörü kullanılarak tüm w liste vektörleri, GaussReduce algoritması tarafından indirgenmektedir. İndirgeme işlemleri bittikten sonra GaussSieve algoritması, indirgenmiş v vektörünün yeni Öklid uzunluğu ile, indirgenmeden önceki uzunluğunu karşılaştırmaktadır. v vektörünün uzunluğunda bir değişiklik yok ise, bu vektör L liste veri yapısında eklenmektedir. Ancak uzunluk değişmiş ve sıfırdan farklı ise v vektörü, S yığınına dâhil edilmektedir. Eğer v vektörünün yeni uzunluğu sıfır ise, cl çakışma sayısı bir arttırılmaktadır ve GaussSieve algoritması yeni bir iterasyona başlamaktadır. cl çakışma sayısı, c maksimum çakışma sayısı ile aynı değere sahip olduğunda ise, GaussSieve algoritması çalışmasını sonlandırmaktadır ve en kısa kafes vektörünü çıktı olarak vermektedir.

GaussSieve algoritması gibi Gauss tabanlı olan ProGaussSieve eleme algoritması, GaussSieve algoritması üzerinde ufak değişiklikler yapılarak geliştirilmiştir. Laarhoven ve Mariano tarafından geliştirilen ProGaussSieve algoritması, GaussSieve algoritmasındaki aynı işlemleri kademeli bir şekilde yapmaktadır. GaussSieve algoritması ile hemen hemen aynı düşünce ve çalışma düzeniyle işlem yapmakta olan ProGaussSieve algoritması, girdi parametresi olarak aldığı kafesi küçük alt parçalara ayırmaktadır ve en küçük alt kafes parçası üzerinde işlem yapmaya başlamaktadır. Buna karşın GaussSieve algoritması ise, tüm kafesi kullanarak çalışmasına başlamaktadır.

Algoritma 1 ProGaussSieve Eleme Algoritması [7]

Girdi İndirgenmiş B kafes bazı, c durdurma kriteri ve $kademe = min\{10, n\}$ sabiti
Çıktı B kafes bazındaki en kısa vektör

$L = \emptyset$
$S = \emptyset$
$cl = 0$
while true **do**
  S yığınından veya Klein'in algoritmasıyla örneklenmiş yeni bir v vektörü getirme
  $GaussReduce(v, w \in L)$
  $GaussReduce(w \in L, v)$
  İndirgenmiş $w \in L$ vektörlerini, L listesinden S yığınına taşıma
  if v sabit **then**
    $L = L \cup \{v\}$
  else
    if $v \neq 0$ **then**
      $S = S \cup \{v\}$
    else
      $cl = cl + 1$
      if $cl = c$ **then**
        if $kademe = n$ **then**
          return $argmin_{v \in L} \|v\|$
        else
          $kademe{+}{+}$
          $cl = 0$

Sözde kodu Algoritma 1'de bulunmakta olan ProGaussSieve algoritması, GaussSieve algoritmasındaki girdi parametrelerine ek olarak, alt kafeslerin boyutlarını belirleyen *kademe* sabitini girdi parametresi olarak almaktadır. *kademe* sabiti ile belirlenen en küçük alt kafes parçası ile işleme başlamakta olan ProGaussSieve algoritması, bu alt kafes parçası üzerinde, GaussSieve algoritmasındaki işlemlerin aynısını yapmaktadır. *cl* çakışma sayısı, *c* durdurma kriterine ulaştığında ise ProGaussSieve algoritması, *kademe* sabitinin değerini arttırarak bir sonraki alt kafes parçası üzerinde işlemine devam etmektedir. Tüm kafes üzerinde işlem yaptıktan sonra ve *kademe* sabiti son seviyede olduğunda ProGaussSieve algoritması, işlemini sonlandırmaktadır ve çıktı olarak en kısa vektörü döndürmektedir.

7.3.1.2. HashSieve Eleme Algoritması

En yakın komşu arama çalışmalarında iyi bilinmekte olan LSH yöntemini kullanmakta olan HashSieve eleme algoritmasının çalışma düzeni ve altındaki ana düşünce, GaussSieve eleme algoritması ile hemen hemen aynıdır. Bu iki eleme algoritmasının birbirinden ayıran en büyük fark, GaussSieve algoritması kafes vektörlerini indirgemek için kullanacağı vektörleri tek bir

liste veri yapısında saklarken, HashSieve algoritması bu liste veri yapısına ek olarak, vektörleri kıyım tablolarında tutmaktadır.

Girdi parametreleri olarak, indirgenmiş B kafesini ve durdurma kriteri c maksimum çakışma sayısını almakta olan HashSieve algoritmasının sözde kodu, Algoritma 2'de verilmektedir. Örnek vektörlerin tutulduğu S yığın veri yapısı ve T kıyım tabloları boş olacak şekilde işleme başlayan HashSieve algoritması bir iterasyonda ilk olarak, S yığın veri yapısından almakta olduğu veya Klein'in En Yakın Komşu algoritmasının üretmekte olduğu yeni bir v örnek vektörünü işleme sokmaktadır. v örnek vektörünü, T kıyım tablolarındaki w en yakın aday vektörleri ile indirgemekte olan HashSieve algoritması, indirgenmiş v vektörü ile tüm w vektörlerini indirgemektedir. Daha sonra HashSieve algoritması, sıfır olmayan indirgenmiş w vektörlerini S yığınına dâhil etmektedir ve sıfır olmayan indirgenmiş v vektörünü T kıyım tablolarına eklemektedir. Eğer indirgenmiş v vektörü sıfır vektör ise HashSieve algoritması, cl çakışma sayısını bir attırmaktadır ve yeni bir iterasyonda işlemine devam etmektedir. cl çakışma sayısı, c durdurma kriterine ulaştığında çalışmasını durduran HashSieve algoritması çıktı olarak, girdi parametresi olarak aldığı kafesin en kısa Öklid uzunluğuna sahip vektörü vermektedir.

Algoritma 2 HashSieve Eleme Algoritması [8]

Girdi İndirgenmiş B kafes bazı ve c durdurma kriteri
Çıktı B kafes bazındaki en kısa vektör

$S = \emptyset$
$cl = 0$
T boş kıyım tabloları $H_1, \ldots, H_T$
while $cl < c$ **do**
  S yığınından veya Klein'in algoritmasıyla örneklenmiş yeni bir v vektörü getirme
  while $\exists w \in H_1[h_1(v)], \ldots, H_T[h_T(v)] : \|v \pm w\| < \|v\|$ **do**
    for each *Kıyım tablo* $H_i, \ldots, H_T$ **do**
      $C = H_i[h_i(v)]$ en yakın aday vektörlerini bulma
      for each $w \in C$ **do**
        w vektörü ile v vektörünü indirgeme ve v vektörü ile w vektörünü indirgeme
        if w değişmiş **then**
          $H_i = H_i / \{w\}$
          if $w = 0$ **then**
            $cl = cl + 1$
          else
            $S = S \cup \{w\}$
  if $v = 0$ **then**
    $cl = cl + 1$
  else
    $H_i = H_i \cup \{v\}$

7.3.1.3. Eleme Algoritmalarının Özelliklerinin Karşılaştırılması

Kafes tabanlı kriptosistemlerdeki en temel zor problemlerden olan SVP problemini çözmek için geliştirilen eleme algoritmaları, hemen hemen aynı çalışma düzeninde ve mantığında işlem yapmaktadırlar. GaussSieve, ProGaussSieve ve HashSieve gibi eleme algoritmaları arasında, kullandıkları veri yapıları farklılıkları veya ufak yöntemsel farklılıklar bulunmaktadır. Eleme algoritmalarındaki bu farklılıklardan dolayı, algoritmaların asimptotik çalışma zamanı ve alan karmaşıklıkları da farklılıklar göstermektedir. GaussSieve, ProGaussSieve ve HashSieve eleme algoritmalarına ait özellikler ve bu algoritmalar arasındaki farklılıklar, Tablo 7.2'de karşılaştırılmıştır [37].

Tablo 7.2. Eleme Algoritmalarının Özelliklerinin Karşılaştırılması [37]

Eleme Algoritmaları	Karmaşıklık (Zaman / Alan)	Mantık	Temel İşlem
GaussSieve	$2^{0.48n}/2^{0.18n}$	Bir liste veri yapısına her bir iterasyonda daha kısa kafes vektörleri dahil etmek	Örnek vektörü tüm liste vektörleri ile indirger ve indirgenen örnek vektör ile tüm liste vektörlerini indirger. Listedeki en kısa vektörü çıktı olarak verir
ProGaussSieve	$2^{0.42n}/2^{0.21n}$	Tüm kafes yerine, kafesi küçük alt parçalara bölmek ve en küçük parça üzerinden işleme başlamak	GaussSieve algoritmasından farklı olarak, durdurma kriterine ulaşana kadar bir kafes parçası üzerinde işlem yapar ve durdurma kriterine ulaşınca, bir sonraki alt parça üzerinde çalışmaya devam eder
HashSieve	$2^{0.3366n}/2^{0.3366n}$	LSH yöntemini kullanmak ve bu yöntem sayesinde aday vektörleri hızlı bir şekilde bulmak	Örnek vektörleri, kıyım tablolarında bulunan en yakın aday vektör ile indirger ve indirgenen örnek vektör ile tüm kıyım tablolarındaki vektörleri indirger. Hedeflenen en kısa vektörü bulana kadar ya da durdurma kriterine ulaşana kadar işlemine devam eder

7.3.2. Numaralandırma Tabanlı Algoritmalar

Bu başlık altında, numaralandırma mantığında çalışmakta olan ENUM numaralandırma algoritmasından ve bu numaralandırma algoritmasını alt işlem olarak kullanmakta olan Schnorr ve Euchner'in BKZ indirgeme al-

goritmasından bahsedilmektedir. Bu algoritmalara ait sözde kodlar verilmektedir ve bu sözde kodlara bağlı olarak algoritmaların çalışma düzenleri anlatılmaktadır.

7.3.2.1. ENUM Numaralandırma Algoritması

Schnorr ve Euchner tarafından önerilmiş ve numaralandırma tabanlı çalışmakta olan ENUM numaralandırma algoritması, SVP probleminden daha çok, Schnorr ve Euchner'in BKZ indirgeme algoritmasında kullanılmak amacıyla geliştirilmiştir. Schnorr ve Euchner'in BKZ algoritmasında alt işlem olarak çalışmakta olan ENUM algoritması, BKZ algoritmasına ait yerel kafes bloğundaki en küçük alanı (vektör) bulmaktadır.

Algoritma 3'te sözde kodu verilmekte olan ENUM algoritması, BKZ algoritmasına entegre olacak şekilde, j ve k indekslerini girdi parametreleri olarak almaktadır. ENUM algoritması, c_j fonksiyonunda bulunmakta olan en küçük $\tilde{c}_j$ için, $\tilde{c}_j > c_t(\tilde{u}_t, \dots, \tilde{u}_k)$ şartını sağlayan tüm $\{\tilde{u}_t, \dots, \tilde{u}_k\}$ tamsayı vektörleri üzerinde derinlemesine bir arama yapmaktadır ve böylece numaralandırma işlemini gerçekleştirmektedir. ENUM algoritması, $\tilde{c}_t > c_t(\tilde{u}_t, \dots, \tilde{u}_k)$ işleminin sonucunu bulduktan sonra, t seviyesinde bulunmakta olan Δ_t ve $\tilde{u}_t$ değişkenlerine 1 değerini vermektedir. s değişkenine, t değişkenin almış olduğu en büyük değeri ayarlayan ENUM algoritması, 1,-1,2,-2,3,-3,… sıralı değerlerden sırası gelen değeri, $\tilde{u}_t \geq \bar{c}_j$ koşulu altında Δ_t değişkenine atamaktadır. İteratif olarak çalışmakta olan ENUM algoritması her bir iterasyonda, s ve t değişkenlerinin değerlerini 1 arttırmaktadır. Daha sonra, $t-1$ seviyesinde çalışmasına devam etmekte olan ENUM algoritması, $-y_t + \lceil -y_t \rfloor$ işleminin sonucunu δ_t değişkenine ve 0 değerini Δ_t değişkenine atamaktadır. Tekrar t seviyesine çıkan ENUM algoritması, 1,-1,2,-2,3,-3,… ya da -1,1,-2,2,-3,3,… sıralı değerlerden sırası gelen değeri, Δ_t değeri olarak ayarlamaktadır. Durdurma kriterine ulaşana kadar işlemlerini iteratif bir şekilde yapmakta olan ENUM algoritması, $\{u_j, \dots, u_k\} \in \mathbb{Z}^{k-j+1}$ en küçük alanı çıktı olarak vermektedir.

Algoritma 3 ENUM Numaralandırma Algoritması [25]

Girdi $1 \leq j < k \leq m$ için j ve k
Çıktı $\{u_j, \ldots, u_k\} \in \mathbb{Z}^{k-j+1}$ en küçük alan

BKZ algoritmasındaki $j \leq t < i \leq k$ için $\mu_{i,t}$, $i = j, \ldots, k$ için $c_i = \|v_i^*\|^2$ değerleri ve $\{v_j, \ldots, v_k\}$ yerel kafes baz vektörleri
$\bar{c}_j = c_j, \tilde{u}_j = u_j = 1, y_j = \Delta_j = 0, s = t = j, \delta_j = 1$
for $i = j + 1$ **to** $k + 1$ **do**
  $\tilde{c}_i = u_i = \tilde{u}_i = y_i = \Delta_i = 0, \delta_i = 1$
while $t \leq k$ **do**
  $\tilde{c}_t = \tilde{c}_{t+1} + (y_t + \tilde{u}_t)^2 c_t$
  if $\tilde{c}_t < \bar{c}_j$ **then**
    if $t > j$ **then**
      $t = t - 1, y_t = \sum_{i=t+1}^{s} \tilde{u}_i \mu_{i,t}$
      $\tilde{u}_t = w_t = \lceil -y_t \rfloor, \Delta_t = 0$
      if $\tilde{u}_t > -y_t$ **then**
        $\delta_t = -1$
      else
        $\delta_t = 1$
    else
      $\bar{c}_j = \tilde{c}_j$
      $i = j, \ldots, k$ için $u_i = \tilde{u}_i$
  else
    $t = t + 1, s = max(s, t)$
    if $t < s$ **then**
      $\Delta_t = -\Delta_t$
    if $\Delta_t \delta_t \geq 0$ **then**
      $\Delta_t = \Delta_t + \delta_t$
      $\tilde{u}_t = w_t + \Delta_t$
return $\{u_j, \ldots, u_k\} \in \mathbb{Z}^{k-j+1}$ en küçük alan

7.3.2.2. Schnorr ve Euchner'in BKZ İndirgeme Algoritması

Kafes indirgemek için kullanılmakta olan ve Schnorr ve Euchner tarafından geliştirilen BKZ algoritması, girdi parametresi olarak aldığı β değeri ile boyutları belirlenen yerel alt kafes blokları üzerinde çalışmaktadır. β parametresine göre indirgeme kalitesi değişmekte olan Schnorr ve Euchner'in BKZ algoritması, kayan nokta (floating-point) hatalarını en aza indirmek için, Schnorr ve Euchner tarafından geliştirilen LLLFP indirgeme algoritmasını [9] alt işlem olarak kullanmaktadır. BKZ algoritmasının bir diğer alt işlem olarak kullandığı algoritma ise, ENUM numaralandırma algoritmasıdır ve yerel kafes bloklarına ait en küçük alanı (vektör) bulmak için kullanılmaktadır.

Schnorr ve Euchner'in BKZ algoritması, n boyutlu L kafesini, $\beta \geq 2$ yerel kafes boyutu değerini, LLLFP indirgeme algoritması için δ kayan nokta hata değerini, Gram-Schmidt μ sabit sayılarını ve indirgenmiş $\|v_1^*\|^2, \ldots, \|v_n^*\|^2$ Gram-Schmidt kafes vektörlerinin boyutlarını girdi parametreleri olarak almaktadır. BKZ algoritmasının bir iterasyondaki ilk işlemi, LLLFP algoritması ile ($F_c = false$ olacak şekilde), β kafesini indirgemektir ve μ sabit sayılarını güncellemektir. $j = 1, \ldots, n$ indeks değerleriyle, $B_{[j,\min(j+\beta-1,n)]}$ yerel kafes bloklarını iteratif bir şekilde indirgeyen BKZ algoritması, j indeksine başlangıç değeri olarak 1 değerini atamaktadır. $u = (u_1, \ldots, u_n)$ en küçük alanı hesaplayabilmek için BKZ algoritması her bir iterasyonda, $k = \min(j + \beta - 1, n)$ indeksinde bulunmakta olan $L_{[j,k]}$ yerel kafesini ENUM algoritmasında işleme sokmaktadır. Yeni yerel kafes bloğunun son indeksi olarak $h = \min(k + 1, n)$ değerini ayarlamakta olan BKZ algoritması, $\|v_j^*\| > \lambda_1(L_{[j,k]})$ koşulu altında $v^{yeni} = \sum_{i=j}^{k} u_i v_i$ yeni kafes vektörünü üretmektedir. BKZ algoritması ürettiği yeni kafes vektörünü, v_{j-1} ve v_j kafes vektörlerinin arasına sokmaktadır. Yeni kafes vektörünün eklenmesiyle, $(v_1, \ldots, v_{j-1}, v^{yeni}, v_j, \ldots, v_h)$ vektörler kümesini elde eden BKZ algoritması, bu vektörler kümesini LLLFP algortimasında işleme sokarak ($(F_c = true)$), yeni $v_1, \ldots, v_h$ indirgenmiş yerel kafes üretmektedir ve μ sabitlerini güncellemektedir. $\|v_j^*\| > \lambda_1(L_{[j,k]})$ koşulu sağlanmıyor ise BKZ algoritması, değişmemiş $v_1, \ldots, v_h$ yerel kafes bloğunu LLLFP algoritmasında işleme sokmaktadır ($(F_c = false)$). Bu işlemler sonucunda, $\{v_1, \ldots, v_h\}$ LLLFP indirgenmiş kafes bazını elde eden BKZ algoritması, j indeksinin değeri n sayısına eşit olduğunda numaralandırma işlemlerinin hepsi başarısız olduysa, 1 değerini j indeksine ayarlamaktadır. İteratif bir şekilde bu işlemlere devam etmekte olan BKZ algoritması, z başarısız numaralandırma işlem sayacını durdurma kriteri olarak kullanmaktadır. Tüm kafes üzerinde işlem yaptıktan sonra ve z durdurma sayacı da $n - 1$ değerine eşit olduğunda BKZ algoritması, çalışmasını durdurmaktadır ve $\{v_1, \ldots, v_n\}$ BKZ indirgenmiş kafesini çıktı olarak döndürmektedir. Schnorr and Euchner'in BKZ algoritmasına ait sözde kod, Algoritma 4'te gösterilmektedir.

Algoritma 4 BKZ İndirgeme Algoritması [9]

Girdi $B = \{v_1, \ldots, v_n\} \in \mathbb{Z}^n$ kafes bazı, $2 < \beta < n$ blok boyutu, $\frac{1}{2} < \delta < 1$ koşuluyla δ, μ sabitleri ve $\|v_1^*\|^2, \ldots, \|v_n^*\|^2$

Çıktı $\{v_1, \ldots, v_n\}$ BKZ indirgenmiş kafes bazı

$z = 0$
$j = 0$
$F_c = false$
$LLLFP(v_1, \ldots, v_n, \delta, F_c)$
while $z < n - 1$ **do**
  $j = (j \, mod(n-1)) + 1$
  $k = min(j + \beta - 1, n)$
  $h = min(k + 1, n)$
  $u = ENUM(j, k)$
  $v^{yeni} = \sum_{i=j}^{k} u_i v_i \quad (\|\pi_j(\sum_{i=j}^{k} u_i v_i)\| = \lambda_1(L_{[j,k]}))$
  if $\|v_j^*\| > \lambda_1(L_{[j,k]})$ **then**
    $z = 0$
    $F_c = true$
    $LLLFP((v_1, \ldots, v_{j-1}, v^{yeni}, v_j, \ldots, v_h), \delta, F_c)$
  else
    $z = z + 1$
    $LLLFP((v_1, \ldots, v_{j-1}, v^{yeni}, v_j, \ldots, v_h), \delta, F_c)$
return $\{v_1, \ldots, v_n\}$ BKZ indirgenmiş kafes bazı

7.4. UYGULAMALAR VE YAZILIM KÜTÜPHANELERİ

Eleme, numaralandırma ve BKZ gibi indirgeme algoritmalarına ait, farklı yazılımsal özelliklere ve yöntemlere dayalı çeşitli uygulamalar geliştirilmiştir. Bu uygulamalar geliştirilirken altyapı olarak, farklı özelliklere sahip yazılım kütüphaneleri kullanılmıştır. Bu bölümde, literatürde önerilen kriptanaliz algoritmalarına ait uygulamalara ve açık kaynak kodlu yazılım kütüphaneleri üzerinde durulmaktadır.

7.4.1. Kriptanaliz Algoritmalarına Ait Uygulamalar

Eleme algoritmalarından olan GaussSieve algoritmasına ait ilk standart uygulama, Micciancio ve Voulgaris tarafından geliştirilmiştir [6]. Bu GaussSieve uygulaması, C++ programlama dili kullanılarak gerçeklenmiştir ve altyapı olarak, açık kaynak kodlu olan NTL yazılım kütüphanesini kullanmaktadır. Satılmış ve Akleylek, kendi geliştirmiş oldukları modüler yazılım altyapı kütüphanesi ile, GaussSieve algoritmasına ait bir başka

standart uygulamayı geliştirmişlerdir [10]. Bu standart GaussSieve uygulamasında durdurma kriteri olarak, işlem sırasında harcanan bellek alanı kullanılmaktadır. Milde ve arkadaşları, GaussSieve algoritmasını paralel yapıya uygun olarak güncellemişlerdir ve pratiğe dönüştürmüşlerdir [19]. Paralel yapılı bu uygulama, işlem sırasında vektörlerin etrafında döndüğü ve her biri bir iş parçacığı (thread) tarafından kontrol edilen, genel bir listenin birkaç parçasını içermekte olan bir halka yapısından oluşmaktadır. GaussSieve algoritmasının bir başka paralel uygulamasını, Ishiguro ve arkadaşları dağıtık-bellek yöntemi kullanarak geliştirmişlerdir [20]. Bu uygulamada, her bir iş parçacığı genel listeye ulaşabildiğinden, vektörlerin listesi iş parçacıkları arasında farklı parçalara bölünmezler. Mariano ve arkadaşları, kilitsiz bağlantılı liste yapısını kullanarak bir diğer paralel yapılı GaussSieve uygulamasını gerçeklemişlerdir [21]. Bu paralel uygulamada vektörler, kilitsiz bağlantılı liste yapısında tutulmaktadır. CPU kullanılarak geliştirilen paralel yapılı bu uygulamalar dışında Yang ve arkadaşları [22], GPU üzerinde paralel GaussSieve uygulamasını geliştirmişlerdir.

GaussSieve eleme algoritması ortaya çıkana kadar, SVP problemini pratik olarak en yaygın şekilde çözmekte olan numaralandırma algoritmalarından en çok ilgi gören ENUM algoritmasına ait bilinen ilk standart uygulamayı, Schnorr ve Euchner tarafından, BKZ algoritmasında alt işlem olarak çalıştırılmak amacıyla geliştirilmiştir [9]. Başarı yüzdesini ve çıktı sonuçlarının kalitesini düşürmek pahasına, hesaplama maliyetinden kaçmak adına bu uygulamada, budama yöntemi kullanılmaktadır. ENUM algoritmasına ait ilk paralel yapılı uygulamayı Dağdelen ve arkadaşları gerçeklemiştir. Bu paralel yapılı uygulama, kullanmakta olduğu çekirdek sayısına göre doğrusal hızlanmalar elde etmektedir. Correia ve arkadaşları, paralel programlama tekniği kullanarak, bir başka paralel yapılı olan numaralandırma uygulamasını gerçeklemişlerdir [28]. SE++ olarak adlandırılan bu uygulama, Dağdelen ve arkadaşları tarafından geliştirilen paralel ENUM uygulamasından daha verimli bir şekilde çalışmaktadır.

İlk kez Schnorr ve Euchner tarafından pratiğe dönüştürülen [9] BKZ indirgeme algoritmasını, Liu ve arkadaşları paralel programlama tekniğini

kullanarak uygulamışlardır [33]. Numaralandırma işlemlerini, farklı yerel kafes blokları üzerinde paralel olarak yapmakta olan bu uygulama, LLL indirgeme algoritmasında kafesin tamamını işleme sokmaktadır. BKZ algoritmasının bir diğer versiyonu olan ACBKZ algoritması, Correia tarafından paralel programlama tekniği kullanılarak geliştirilmiştir [34]. ACBKZ algoritmasına ait paralel uygulama, alt işlem olarak kullanmakta olduğu numaralandırma algoritmasını, paralel olarak farklı bloklar üzerinde işleme sokmaktadır.

7.4.2. Yazılım Kütüphaneleri

Kriptanaliz algoritmalarına ait standart veya paralel yapılı uygulamaları geliştirmek için, altyapı olarak kullanılmak amaçlı yazılım kütüphanelerine ihtiyaç duyulmaktadır. Kriptanaliz algoritmalarında alt işlem olarak kullanılmakta olan bileşenleri ve yöntemleri içermekte olan bu yazılım kütüphanelerinin bir kısmı açık kaynak kodlu olarak bulunmaktadır.

Kafes tabanlı kriptografi alanında mevcut olan en önemli ve en popüler yazılım kütüphanelerinin başında, fplll açık kaynak kodlu yazılım kütüphanesi gelmektedir. C++ programlama dili kullanılarak geliştirilen fplll yazılım kütüphanesi, LLL algoritmasına ait kayan nokta hataları için geliştirilmiş (LLLFP) algoritmaların verimli uygulamalarını içermektedir. BKZ algoritmasının farklı versiyonlarının (BKZ 2.0) verimli uygulamalarını da barındırmakta olan fplll kütüphanesi, çeşitli eleme (GaussSieve) ve numaralandırma uygulamalarının kullanılmasına da imkân sağlamaktadır. fplll kütüphanesi ayrıca, CVP probleminin çözümü için bir numaralandırma algoritması da sağlamaktadır.

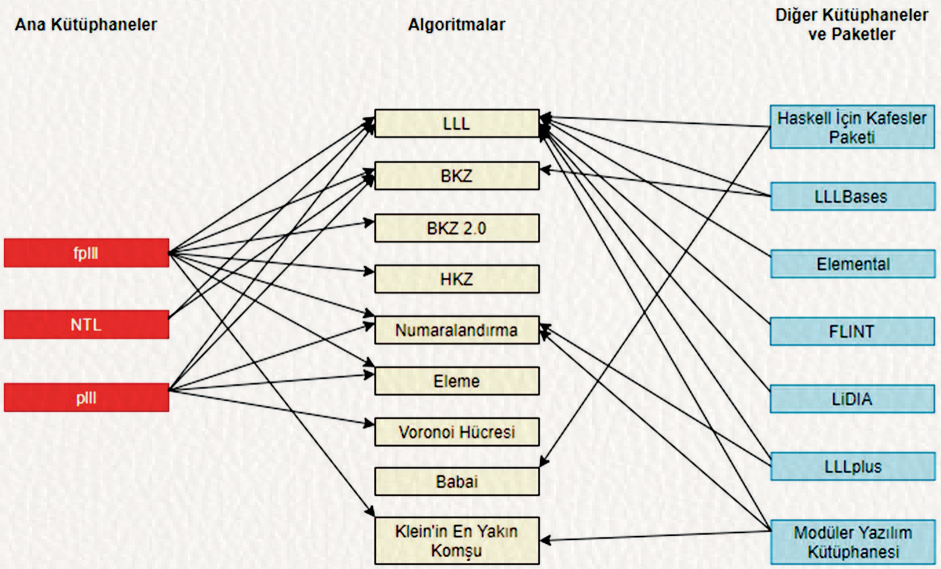
fplll yazılım kütüphanesini geliştirilmeden önce en çok ilgi görmekte olan NTL açık kaynaklı yazılım kütüphanesi, C++ programlama dili kullanılarak geliştirilmiştir. Bu yazılım kütüphanesi, kafes tabanlı kriptografi alanı için, LLL ve BKZ algoritmalarının pratik olarak kullanılmasına olanak sağlamaktadır. NTL yazılım kütüphanesi, yüksek hassasiyet ile işlem yapılmasına izin vermektedir ve bu sayede elde edilen çıktılarda oluşan hata oranlarını en aza indirmektedir.

fplll ve NTL yazılım kütüphaneleri dışında plll kütüphanesi, C++ programlama dili üzerinde gerçekleşmiştir. plll yazılım kütüphanesi içerisinde, LLL, BKZ ve SVP problemini çözmekte olan algoritmalara ait çeşitli uygulamaları barındırmaktadır. Bu yazılım kütüphanesi, LLL indirgeme algoritmasının klasik ve Siegel [38] gibi versiyonlarının uygulamalarını içermektedir. Bir diğer indirgeme algoritması olan BKZ algoritmasının Schnorr ve Euchner, Primal-Dual [39] gibi çeşitlerine ait uygulamaları sağlamakta olan plll yazılım kütüphanesi, Kannan-Schnorr-Euchner numaralandırma algoritmasının uygulamasını sunmaktadır. Bu yazılım kütüphanesinde, ListSieve eleme algoritmasının çeşitleri ile birlikte, GaussSieve eleme algoritması da bulunmaktadır.

Bir diğer açık kaynak kodlu yazılım kütüphanesi olan modüler yazılım altyapı kütüphanesi [14], C programlama dili kullanılarak geliştirilmiştir. Modüler yazılım kütüphanesi içerisinde, kriptanaliz uygulamalarının geliştirilmesi için kullanılabilecek Gram-Schmidt, LLL, LLLFP, GaussReduce, ENUM, Klein'in En Yakın Komşu (nearA [35] ve randRound [40]) algoritmalarının temel versiyonlarına ait modüller bulunmaktadır. 64-bit mimariye uygun olarak tasarlanmış bu yazılım kütüphanesi kullanılarak, GaussSieve, ProGaussSieve, HashSieve ve Schnorr ve Euchner'in BKZ algoritmalarına ait verimli uygulamalar geliştirilmiştir ve bu uygulamalar kütüphane içerisinde çalıştırılabilir bir program olarak bulunmaktadırlar [14].

Kriptanaliz algoritmalarına ait uygulamaların geliştirilmesi için kullanılabilecek başka yazılım kütüphaneleri de bulunmaktadır. Bu yazılım kütüphanelerinden, Babai En Yakın Düzlemler algoritmasına [41] ait uygulamayı içermekte olan Haskell için kafesler paketi kütüphanesi [42], temel LLL algoritmasına ve LLLFP algoritmasına ait uygulamaları bulundurmaktadır. LLL algoritmasının çeşitli versiyonlarına ve BKZ algoritmasına ait uygulamaları, LLLBases isimli bir paket içerisinde barındırmakta olan MACAULAY2 yazılım kütüphanesi [43], bu uygulamaları farklı hassasiyet oranlarında kullanımına olanak sağlamaktadır. Doğrusal cebir ve kafes indirgemesi için hazır yapılar sağlamakta olan ve C++ programlama dili ile geliştirilmiş temel yazılım kütüphanesi [44], LLL algoritmasını ve çeşitli kafes örneklerini sunmaktadır. C programlama dili ile yazılmış ve sayılar teorisi

yazılım kütüphanesi olan FLINT [45], optimize edilmiş LLL algoritmasına ait uygulamayı bulundurmaktadır. Bir başka LLL uygulamasını içermekte olan LiDIA yazılım kütüphanesi [46], hesaplamalı sayılar teorisinde kullanılmaktadır ve C++ programlama dili ile geliştirilmiştir. LLL ve SVP/CVP problemlerinin çözümü için numaralandırma uygulamalarını içermekte olan LLLplus yazılım kütüphanesi [47], Julia üzerinden gerçeklenmiştir. Şekil 7.1'de, yazılım kütüphanelerinde bulunmakta olan başlıca temel kriptanaliz uygulamaları gösterilmektedir.



Şekil 7.1. Yazılım kütüphanelerinin ve paketlerinin içerdikleri başlıca uygulamalar ve bileşenler

7.5. SONUÇ VE DEĞERLENDİRMELER

Kuantum sonrası dönem için güvenli olduğu düşünülmekte olan kafes tabanlı kriptosistem ailesinde, kriptanaliz yöntemi olarak kullanılmakta olan GaussSieve, ProGaussSieve ve HashSieve eleme algoritmalarına ait olan ana düşüncelerin ve bu algoritmaların çalışma düzenlerinin üzerinde du-

rulmuştur. Bu eleme algoritmalarının karmaşıklık değerleri, mantıkları ve temel işlemleri Tablo 7.2'de sunulmuştur. Tablo 7.2 göz önüne alındığında, en düşük çalışma zamanına sahip olan algoritma HashSieve algoritmasıyken, en düşük bellek alanı kullanan algoritmanın ise GaussSieve algoritması olduğu görülmüştür.

Kriptanaliz algoritmalarına ait uygulamaların geliştirilebilmesi için yazılım kütüphanelerine gereksinim duyulmaktadır. Bu nedenden dolayı, kriptanaliz algoritmalarında ortak olarak bulunmakta olan yapıları ve alt algoritmaları uygulama şeklinde içermekte olan, birçok yazılım kütüphanesi geliştirilmiştir. Bu yazılım kütüphanelerinin başlıca hangi temel uygulamaları içerdikleri, Tablo 7.1 ve Şekil 7.1'de özetlenmiştir. Tablo 7.1 ve Şekil 7.1 incelendiğinde, açık kaynak kodlu olan fplll ve plll yazılım kütüphanelerinin, en zengin içeriğe sahip olan kütüphaneler oldukları gözlemlenmiştir. Bu yazılım kütüphaneleri, özellikle fplll kütüphanesi, zengin içeriklerinden dolayı çok ilgi görmektedirler. Bir diğer yazılım kütüphanesi olan NTL kütüphanesinin, birçok uygulamada altyapı olarak kullanıldığı ve hassas hesaplama özelliği olduğu görülmüştür. Kriptanaliz uygulamalarının geliştirilebilmesi için, alt işlem olarak kullanılmakta olan yapıları ve algoritmaları modüler yapıda içermekte olan modüler yazılım kütüphanesinin ise, birçok verimli uygulamada altyapı olarak kullanıldığı görülmüştür. İncelenen diğer yazılım kütüphanelerinin ve paketlerinin içerisinde ise, çoğunlukla LLL algoritmasına ait çeşitli uygulamaların bulunduğu sonucuna ulaşılmıştır.

Teşekkür

Bu bölüm, EEEAG-117E636 proje numarası ile TÜBİTAK tarafından desteklenmiştir.

KAYNAKLAR

[1] P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in: Proceedings 35th annual symposium on foundations of computer science, Ieee, 1994, pp. 124–134.

[2] D. J. Bernstein, Introduction to post-quantum cryptography, in: Post-quantum cryptography, Springer, 2009, pp. 1–14.

[3] L. Chen, L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, D. Smith-Tone, Report on post-quantum cryptography, Vol. 12, US Department of Commerce, National Institute of Standards and Technology, 2016.

[4] S. Akleylek, M. Soysaldı, Kuantum bilgisayarlar ile kriptoanaliz ve kuantum sonrası güvenilir kripto sistemleri, Sağıroğlu, M. Şenol (Eds.), Siber Güvenlik ve Savunma: Farkındalık ve Caydırıcılık Cilt II, Grafiker Yayınları, pp. 137–168.

[5] S. Akleylek, K. Seyhan, Kuantum bilgisayarlar sonrası güvenilir kafes tabanlı kriptosistem temellerine giriş, in: e. Sağıroğlu, M. Şenol (Eds.), Siber Güvenlik ve Savunma: Farkındalık ve Caydırıcılık Cilt II, Grafiker Yayınları, pp. 171–209.

[6] D. Micciancio, P. Voulgaris, Faster exponential time algorithms for the shortest vector problem, in: Proceedings of the twenty-first annual ACM-SIAM symposium on Discrete Algorithms, SIAM, 2010, pp. 1468–1480.

[7] T. Laarhoven, A. Mariano, Progressive lattice sieving, in: International Conference on Post-Quantum Cryptography, Springer, 2018, pp. 292–311.

[8] T. Laarhoven, Sieving for shortest vectors in lattices using angular locality-sensitive hashing, in: Annual Cryptology Conference, Springer, 2015, pp. 3–22.

[9] C.-P. Schnorr, M. Euchner, Lattice basis reduction: Improved practical algorithms and solving subset sum problems, Mathematical programming 66 (1-3) (1994) 181–199.

[10] H. Satilmis, S. Akleylek, Efficient implementations of gauss-based sieving algorithms, in: Proceedings of the IEEE 28th Signal Processing and Communications Applications Conference, 2020., IEEE, 2020.

[11] fplll yazılımcıları, The fplll lattice reduction library (2008 (Erişim tarihi: 18.05.2020)). URL https://github.com/fplll/fplll

[12] V. Shoup, vd., Ntl: A library for doing number theory (2001), URL http: //www. shoup. net/ntl.

[13] plll yazılımcıları, The plll lattice reduction library (2011 (Erişim tarihi: 18.05.2020)). URL https://felix.fontein.de/plll/

[14] H. Satılmış, S. Akleylek, Modular software library (2020 (Erişim tarihi: 20.05.2020)). URL https://github.com/hsatilmis/modular software library

[15] T. Laarhoven, B. de Weger, Faster sieving for shortest lattice vectors using spherical locality-sensitive hashing, in: International Conference on Cryptology and Information Security in Latin America, Springer, 2015, pp. 101–118.

[16] M. Ajtai, R. Kumar, D. Sivakumar, A sieve algorithm for the shortest lattice vector problem, in: Proceedings of the thirty-third annual ACM symposium on Theory of computing, 2001, pp. 601–610.

[17] P. Q. Nguyen, T. Vidick, Sieve algorithms for the shortest vector problem are practical, Journal of Mathematical Cryptology 2 (2) (2008) 181–207.

[18] A. Mariano, C. Bischof, T. Laarhoven, Parallel (probable) lock-free hash sieve: A practical sieving algorithm for the svp, in: 2015 44th International Conference on Parallel Processing, IEEE, 2015, pp. 590–599.

[19] B. Milde, M. Schneider, A parallel implementation of gausssieve for the shortest vector problem in lattices, in: International Conference on Parallel Computing Technologies, Springer, 2011, pp. 452–458.

[20] T. Ishiguro, S. Kiyomoto, Y. Miyake, T. Takagi, Parallel gauss sieve algorithm: Solving the svp challenge over a 128-dimensional ideal lattice, in: International Workshop on Public Key Cryptography, Springer, 2014, pp. 411–428.

[21] A. Mariano, S. Timnat, C. Bischof, Lock-free gausssieve for linear speedups in parallel high performance svp calculation, in: 2014 IEEE 26th International Symposium on Computer Architecture and High Performance Computing, IEEE, 2014, pp. 278–285.

[22] S.-Y. Yang, P.-C. Kuo, B.-Y. Yang, C.-M. Cheng, Gauss sieve algorithm on gpus, in: Cryptographers' Track at the RSA Conference, Springer, 2017, pp. 39–57.

[23] R. Kannan, Improved algorithms for integer programming and related lattice problems, in: Proceedings of the fifteenth annual ACM symposium on Theory of computing, 1983, pp. 193–206.

[24] U. Fincke, M. Pohst, A procedure for determining algebraic integers of given norm, in: European Conference on Computer Algebra, Springer, 1983, pp. 194–202.

[25] C.-P. Schnorr, M. Euchner, Lattice basis reduction: Improved practical algorithms and solving subset sum problems, in: International Symposium on Fundamentals of Computation Theory, Springer, 1991, pp. 68–85.

[26] N. Gama, P. Q. Nguyen, O. Regev, Lattice enumeration using extreme pruning, in: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2010, pp. 257–278.

[27] Ö. Dagdelen, M. Schneider, Parallel enumeration of shortest lattice vectors, in: European Conference on Parallel Processing, Springer, 2010, pp. 211–222.

[28] F. Correia, A. Mariano, A. Proenca, C. Bischof, E. Agrell, Parallel improved schnorr-euchner enumeration for the cvp and svp, in: 2016 24th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing (PDP), IEEE, 2016, pp. 596–603.

[29] P. Q. Nguyen, B. Vallee, The LLL algorithm, Springer, 2010.

[30] H. W. Lenstra, A. K. Lenstra, L. Lovasz, vd., Factoring polynomials with rational coeficients.

[31] G. Hanrot, X. Pujol, D. Stehle, Analyzing blockwise lattice algorithms using dynamical systems, in: Annual Cryptology Conference, Springer, 2011, pp. 447–464.

[32] Y. Chen, P. Q. Nguyen, Bkz 2.0: Better lattice security estimates, in: International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2011, pp. 1–20.

[33] X. Liu, X. Fang, Z. Wang, X. Xie, A new parallel lattice reduction algorithm for bkz reduced bases, Science China Information Sciences 57 (9) (2014) 1–10.

[34] F. J. G. Correia, Assessing the hardness of svp algorithms in the presence of cpus and gpus, Ph.D. thesis (2014).

[35] P. Klein, Finding the closest lattice vector when it's unusually close, in: Proceedings of the eleventh annual ACM-SIAM sympo- sium on Discrete algorithms, 2000, pp. 937–941. :2020:6052020:605:2020:605:2020:605

[36] A. Mariano, Lusa: the hpc library for lattice-based cryptanalysis, Cryptology ePrint Archive, Report 2020/605 (2020). URL https://eprint.iacr.org/2020/605

[37] S. Akleylek, H. Satılmış, Parameter estimation for lattice-based cryptosystems by using sieving algorithms, in: 2019 4th Interna- tional Conference on Computer Science and Engineering (UBMK), IEEE, 2019, pp. 372–377.

[38] C. L. Siegel, Lectures on the Geometry of Numbers, Springer Science & Business Media, 2013.

[39] D. Micciancio, M. Walter, Practical, predictable lattice basis reduction, in: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2016, pp. 820–849.

[40] P. Raghavan, C. D. Tompson, Randomized rounding: a technique for provably good algorithms and algorithmic proofs, Combi- natorica 7 (4) (1987) 365–374.

[41] L. Babai, On lovasz'lattice reduction and the nearest lattice point problem, Combinatorica 6 (1) (1986) 1–13. [42]B. Coppens, Lattices: A library for lattices (2018 (Erişim tarihi: 20.05.2020)). URL https://hackage.haskell.org/package/Lattices

[43] D. Grayson, M. Stillman, D. Eisenbud, Macaulay2 (1992 (Erişim tarihi: 20.05.2020)). URL http://www2.macaulay2.com/Macaulay2/

[44] E. S. L. Developers, Elemental software library (2016 (Erişim tarihi: 20.05.2020)). URL https://github.com/elemental/Elemental

[45] W. Hart, FLINT: Fast Library for Number Theory (2016 (Erişim tarihi: 20.05.2020)). URL http://www.flintlib.org/

[46] J. B. Group, LiDIA — A library for computational number theory (1994 (Erişim tarihi: 20.05.2020)). URL https://github.com/mkoeppe/LiDIA

[47] C. Peel, LLLplus Software Library (2015 (Erişim tarihi: 20.05.2020)). URL https://github.com/christianpeel/LLLplus.jl

Bölüm 8

AĞ ANOMALİ TESPİTİNDE MAKİNE ÖĞRENMESİ ALGORİTMALARININ KULLANILMASI VE SINIFLANDIRMA İÇİN BİR UYGULAMA ÖRNEĞİ

Habibe Güler - Şeref Sağıroğlu

Günümüzde gelişen teknoloji hayatımızın birçok farklı alanında bizlere kolaylık sağlamasının yanı sıra beraberinde birtakım tehlikeler de getirmektedir. Artan teknoloji kullanımıyla birlikte bilgilerimizde dijital ortama yani diğer bir değişle siber uzaya taşınmıştır. Bunun akabinde ise değerli bilgilerimizi ele geçirmek, onlara ulaşmamızı engellemek içinde saldırganlar boş durmamaktadır. Özellikle casus yazılımlar vasıtasıyla gerçekleşen siber saldırılar her geçen gün giderek yaygınlaşmaktadır. Saldırganlar tarafından gerçekleştirilen bu eylemler normal seyrinde ilerleyen sistemlerimizde birtakım anormal değişikliklere sebep olmaktadır. Sistemlerin korunmasında bu anormalliklerin tespit edilmesi büyük önem arz etmektedir. Temel olarak anomali tespiti bir sistemdeki veya verideki beklenmedik durum veya desenlerin bulunmasını sağlayan teknikler ile bütüncül bir bakış açısıyla gerçekleştirilir. Anomali tespiti yaklaşımı günümüzde ağ saldırı tespiti, sahtekârlık veya dolandırıcılık tespiti, endüstriyel casusluk veya hasar tespiti gibi birçok alanda uygulanmaktadır. Bu kapsamda ise ağlar üzerinde anomali tespitinde makine öğrenmesi algoritmaları bu bölümde incelenmiş, yapılan uygulama çalışması ile de algoritmaların başarıları karşılaştırılmıştır.

8.1. GİRİŞ

Son on yıldır bilgi işlem ve iletişim teknolojileri (BİT), özelde, kamuda ve sektörde yaygın olarak kullanılmaya başlamıştır. Teknolojide meydana gelen gelişmeler, insanların farklı birçok iletişim aracını güvenerek kullanması noktasında büyük artışa sebep olmuştur. Kullanıcılar, şirketler ve hükümetler, günlük faaliyetlerini yürütmek için internet hizmetlerinin yanı sıra diğer cihazlara ve uygulamalara da bağımlı hâle gelmiştir. Bu durum sanal ve fiziksel dünya arasındaki hızlı ve etkili bir yönetim gerekliliğini açıkça göstermektedir. Söz konusu teknolojiler bizler için önemli ölçüde fayda sağlarken, aynı zamanda sürekli olarak çeşitli yeni güvenlik açıkları oluşturan ciddi siber saldırı tehditleriyle de karşı karşıyadırlar. Saldırganlar tarafından gerçekleştirilen bu saldırılar normal seyrinde ilerleyen sistemlerimizde birtakım anormal değişikliklere sebep olmaktadır. Sistemlerin korunmasında bu anormalliklerin tespit edilmesi büyük önem arz etmektedir. Temel olarak anomali tespiti bir sistemdeki veya verideki beklenmedik durum, desen veya örüntülerin bulunmasını sağlayan teknikler bütünüdür. Anomali tespiti yaklaşımı günümüzde ağ saldırı tespiti, dolandırıcılık tespiti, endüstriyel casusluk ve yıkım tespiti gibi birçok alanda uygulanmaktadır.

Bu çalışmanın amacı;

- siber saldırılar içinde büyük bir orana sahip olan ağ tabanlı saldırıların tespit edilmesinde ağlarda anomali tespiti yaklaşımı kullanılarak sistemlerin güvenliğini sağlamak,
- olası tehditlere karşı önceden tedbir alabilme noktasında sistemlerin geliştirilmesine katkıda bulunmak,
- danışmanlı öğrenme sınıflandırma yaklaşımı kullanan makine öğrenmesi algoritmaları kullanılarak sınıflandırma öreği sunmak,
- söz konusu algoritmaların bir takım performans metrikleri kullanılarak karşılaştırılması ve en optimal çözümün seçilmesi ve
- bu deneyimlerin paylaşılarak bu konularda çalışmalar yapacak olanlar ile paylaşılması olarak

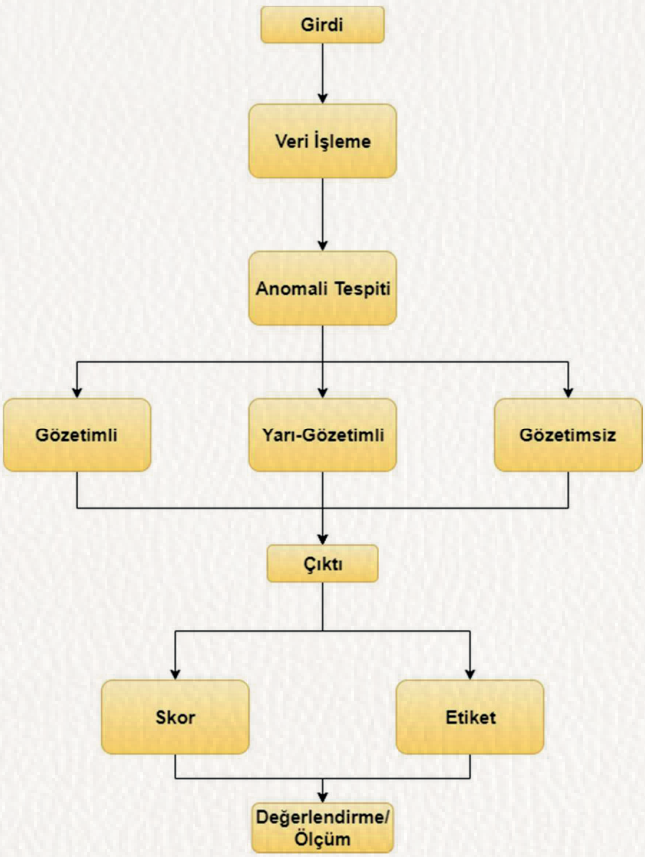
hedeflenmektedir.

Ağlarda anomali tespitinde kullanılacak veriler çok büyük boyutlarda ve anlamlandırılması zor olabilmektedir. Bu sebeple öncelikle, veri kümelerinin

çalışma kapsamında belirlenen hedef doğrultusunda düzenlenmesi ve verilerin belli bir ölçeğe uygun hâle getirilmesi gerekmektedir. Ağ saldırı tespiti noktasında anormalliklerin sağlıklı bir şekilde tespit edilebilmesinde kullanılan algoritmaların doğru parametreler verilerek uygulanması büyük önem arz etmektedir. Fakat söz konusu makine öğrenmesi algoritmalarının veri kümesi üzerinde aynı performansı göstermesi beklenmemelidir. Bu sebeple elimizde bulunan veri kümesine en uygun algoritmayı seçme noktasında birtakım performans metriklerine bakılarak karşılaştırılma yapılması gerekmektedir. Bu çalışma kapsamında öncelikle konu ile ilgili literatür taraması yapılarak gerekli teorik altyapının araştırılması, anlaşılması ve elimizde bulunan veri kümesine en uygun sınıflandırma algoritmasına karar verebilmek amacıyla mevcut algoritmaların karşılaştırılması yapılmış olup daha sonra seçilen algoritma ile çalışma hedefi gerçekleştirilmiştir. Çalışmanın ikinci başlığında anomali tespiti kuramsal olarak irdelenmiş, üçüncü başlıkta uygulamanın gerçekleştirilmesinde kullanılacak araç ve makine öğrenmesi algoritmalarından detaylı bir şekilde bahsedilerek metodoloji tanımlanmış, dördüncü başlıkta uygulamanın nasıl gerçekleştirildiği, kullanılan veri seti ve algoritmaların deneysel karşılaştırılmasına yer verilmiş, son olarak ise sonuç ve öneriler kısmı ile çalışma sonlandırılmıştır.

8.2. AĞLARDA ANOMALİ TESPİTİ VE SALDIRI TESPİT SİSTEMLERİ

Anomali tespiti için kullanılan bir veri setindeki anormallikleri yani beklenmedik durum veya desenleri tespit eden bir veri analizi yaklaşımıdır ve verideki nadir desenlerin keşfedilmesine odaklandığından veri madenciliği araştırmalarının da ilgi alanına girmektedir [1]. Aykırı değer tespiti (outlier detection), yenilik algılama (novelty detection), sapma tespiti (deviation detection), istisna madenciliği (exception mining) gibi birçok isimle de eş anlamlı olarak kullanılabilen anomali tespiti günümüzde istatistik ve makine öğrenmesi alanlarında yaygın olarak çalışılmaktadır ve özellikle ağ saldırılarının tespit edilmesinde de önemli fayda sağlamaktadır. Şekil 8.1'de ağlarda anomali tespitinin genel çerçevesi özetlenmiştir. Ek olarak konunun daha iyi anlaşılabilmesi için bu çalışma kapsamında tür, kullanılan yaklaşımlar ve kullanım alanları açısından anomali tespiti detaylı olarak alt başlıklarda incelenecektir.



Şekil 8.1. Ağlarda anomali tespitinin genel çerçevesi [1,2]

8.2.1. Anomali Türleri

Nokta (point), bağlamsal (contextual) ve kolektif (collective) olmak üzere üç tip anomali vardır.

- **Nokta anomali (Point anomaly):**

Belirli bir veri örneği veri kümesinin normal modelinden saptığında yani veri kümesinin geri kalanından farklı bir davranış sergiliyorsa, bu bir nokta anomalisi olarak kabul edilir [1, 3]. Burada bu anomali tespitine nokta anomali denmesinin sebebi anomali tespitinin belli bir niteliğe veya özelliğe (attribute) bağlı olmasıdır. Her ay düzenli olarak 500 liralık alışveriş yapan birisinin

rastgele bir ayda 20 bin liralık alışveriş yapması nokta anomaliye gerçek hayattan verilebilecek iyi bir örnektir.

- **Bağlamsal anomali (Contextual anomaly):**

Eğer bir veri örneği belirli bir bağlam içinde anormal ise, o zaman bağlamsal veya koşullu anomali olarak adlandırılır [1,3]. Örneğin, bayram gibi önemli gün ve haftaların olduğu zamanlarda yapılan harcamalar yılın geri kalan zamanından daha yüksek olmaktadır. Yapılan bu masraflar yüksek miktarda olsa bile bağlamsal olarak normal kabul edilebilir fakat böyle zamanların dışında bir ay boyunca eşit derecede yüksek bir harcama, bağlamsal bir anomali olarak kabul edilebilir [1].

- **Kolektif anomali (Collective anomaly):**

Birbiriyle ilişkili veya benzer olan verilerin koleksiyonu tüm veri kümesine göre anormal davranış oluşturuyorsa kolektif anomali olarak adlandırılır [1-3]. Burada ilişkili olan bazı veriler bir araya geldiğinde anomali oluşturabilirken, veri setinde bu veriler bireysel olarak bulunduğunda anomali olarak kabul edilmezler. Örneğin, bir insanda Elektro Kardiyogram (EKG) çıkışında, uzun bir süre düşük değerlerin varlığı, anormal bir olgunlaşma öncesi kasılmaya karşılık gelen bir dış fenomeni gösterirken, tek başına düşük bir değer anormal kabul edilmez [4].

8.2.2. Anomali Tespit Tekniklerinin Çıktıları

Anormalliklerin veya aykırılıkların raporlanma şekli, herhangi bir anomaliyi tespit tekniği için önemli unsurlardan biridir. Bu açıdan bakıldığında, anomali tespitinin çıktılarını temsil etmenin iki temel yolu vardır. Bunlar skorlar ve etiketlerdir.

- Skor: Puanlama tabanlı anomali algılama teknikleri, her veri örneğine o örneğin anomali şeklinde değerlendirilme derecesine bağlı olarak bir anomali puanı atar [1,2]. Daha sonra skorlar sıralanır ve bir analist anomalileri seçer veya seçmek için bir eşik kullanır [1].
- İkili/etiket: Bu yaklaşımda, her veri örneğine bir etiket (normal ve anormal) değeri atanır [2]. Bu yöntemde veri örnekleri ikili yaklaşımla etiketlenmiş olur yani bir veri örneği normal veya anormal olmak üzere iki farklı değerden ancak birini alabilir.

Puanlamaya dayalı anomali tespit teknikleri analistin en alakalı anomalileri seçmek için alana özel bir eşik kullanmasına izin verirken etiketlemeye dayalı tekniklerde bu mümkün değildir. Buna karşılık ikili etiket yaklaşımını kullanan tekniklerde, her veri örneğinin bir anormallik puanı sağlaması gerekmediğinden bu teknik hesaplama açısından daha verimlidir.

8.2.3. Anomali Tespitinde Kullanılan Yöntemler

Literatüre bakıldığında anomali tespitinde yaygın olarak kullanılan makine öğrenmesi teknikleri bazılarında [5-7] danışmanlı, yarı danışmanlı veya danışmansız öğrenme tabanlı olmak üzere üç temel başlıkta irdelenirken diğerlerinde ise [1-3]; istatistiksel anomali tespiti, kümeleme tabanlı anomali tespiti, bilgi kuramsal anomali tespiti, sınıflandırma tabanlı anomali tespiti olmak üzere dört başlıkta incelenmektedir. Söz konusu tüm bu yöntemleri daha detaylı aşağıda madde madde incelendiğinde;

- Danışmanlı öğrenme modeli ile anomali tespitinde, model sınıf etiketine sahip verileri kullanarak öğrenme işlemini gerçekleştirir. Anomali tespitinde modeli eğitmek için kullanılacak veri setindeki her bir veri örneği bir takım özniteliklere ve sınıf etiketine sahip olmaktadır [5]. Danışmanlı öğrenme algoritmalarının temel yaklaşımlarından biri, girdi özellikleri ve tahmini hedef çıktıları arasındaki ilişkileri ve bağımlılık bağlantılarını temsil eden modeli oluşturmaktır [7]. Sisteme birtakım girdi ve sınıf etiketine sahip çıktılar sağlanır ve sistem öğrenirken veri ve sınıfları arasındaki ilişki modelini kurar [6, 7]. Söz konusu danışmanlı öğrenme algoritmaları öğrenme işlemini sınıflandırma veya regresyon olmak üzere iki farklı şekilde gerçekleştirebilmektedir. Sınıflandırma probleminde model kategorik değerlerin bir sınıfa atanmasıyla ilgilenirken, regresyon probleminde ise süreklilik gösteren değerlerin tahmin edilebilmesi söz konusudur. Destek Vektör Makinesi, Navie Bayes, En Yakın Komşu, Yapay Sinir Ağları, Karar Ağaçları, Rastgele Orman algoritmaları bilinen en yaygın danışmanlı öğrenme algoritmaları olarak söylenebilir [5-7].
- Yarı danışmanlı öğrenme modelinde ise isminden anlaşılacağı üzere hem etiketli hem de etiketsiz veriler ile çalışılmaktadır gerçek hayat problemlerinde de olduğu gibi. Yarı danışmanlı öğrenmede iki temel amaç vardır. Bunlar; eğitim setindeki etiketlenmemiş veriler üzerin-

deki etiketleri tahmin etmek ve gelecekteki test veri setlerinde etiketleri tahmin etmektir [7].

- Danışmansız öğrenme yaklaşımında girdilerle ilişkili etiketlendirilmiş çıktı verileri yoktur algoritmalar etiketsiz verilerle çalışır. Bu yaklaşımın kullanım amacı benzer örüntüleri kümeler hâlinde sınıflandırmak, boyut azaltma ve verilerden anormallik tespiti yapmaktır [6,7]. Danışmansız öğrenme algoritmaları kümeleme ve boyut azaltma olmak üzere iki temel yaklaşım kullanırlar [5-7]. K-ortalama ve Temel Bileşen Analizi sırasıyla bilinen en yaygın kümeleme ve boyut azaltma yöntemleri olarak söylenebilir.
- İstatistiksel anomali tespiti tekniğinde öncelikle normal verilerden bir istatistiksel model oluşturulur. Sonrasında daha önceden karşılaşılmamış verilerin bu modele ait olup olmadığı test edilir. İstatistiksel yaklaşımın karışım modeli (mixture model), sinyal işleme (signal processing) ve temel bileşen analizi (PCA) olmak üzere üç türünden bahsedilebilir. Karışım modelleri bir popülasyona ait alt popülasyonları tanımlarken olasılıklarla temsil edilmesi esasına dayanır. Anomali tespiti açısından düşündüğümüzde veri örneklerindeki normal ve anormal dağılımların belli bir olasılık katsayısına sahip olması ve bu katsayıların bu örneklerle çarpımlarının toplamının tüm veriyi temsil etmesi şeklinde tanımlanabilir. Eskin ve arkadaşları [8] çalışmalarında bu yöntemi kullanmışlardır.
- Kümeleme tabanlı anomali tespiti ise veri kümesindeki noktalar herhangi bir sınıf etiketine sahip değilse uygulanmaktadır. Farklı birçok kümeleme tekniği olmakla beraber bu çalışma kapsamında düzenli kümeleme (regular clustering) ve ortak kümeleme (co-clustering) olmak üzere iki tip kümelemeden ağ anomali tespitinde kullanışlı olması sebebiyle bahsetmek gerekmektedir [1]. Bu iki yaklaşım satır ve sütunları işlerken farklı teknikler kullanmaktadır. Örneğin, k-ortalamalar kümeleme yaklaşımı bir düzenli kümeleme türüdür ve kümeleme sırasında veri setinin satırlarını yani gözlemlerini dikkate alır [1]. Ortak kümelemede ise kümeleme yaparken veri setinin hem satır hem de sütunları dikkate alınarak kümeleme yapılmaktadır. Bu bağlamda temel bir anlayış ile düşünüldüğünde normal olan noktalar kendi aralarında birer küme oluştururken bu kümelerin dışında kalan noktaların ise anormal olduğu tespit edilmiş olur.

- Bilgi kuramsal anomali tespiti yaklaşımı uygun bir anomali tespit modeli oluşturmak için kullanılabilir [1]. Bu teknikler, bir veri kümesinin bilgi içeriğini Kolmogorov Karmaşıklığı, entropi, bağıl entropi ve benzeri gibi farklı bilgi teorik ölçümlerini kullanarak analiz eder [2]. Burada anomali tespitinde temel varsayım verilerdeki anormalliklerin, veri kümesinin bilgi içeriğindeki düzensizlikleri tetiklemesidir. Söz konusu bu yöntemlerde, ağ veya ana bilgisayar olayları önceden tanımlanmış kurallara veya saldırı modellerine göre kontrol edilirler [3].
- Sınıflandırma tabanlı anomali tespitinde kümeleme tabanlı yaklaşımın aksine veri kümesindeki noktalar sınıf etiketine sahiptir. Eğitim ve test olmak üzere iki aşamada veriler sınıflandırılır. Öncelikle eğitim aşamasında model mevcut etiketli eğitim verilerini kullanarak bir sınıflandırıcıyı öğrenir. Test aşamasında ise model bir test örneğini öğrendiği sınıflandırıcıyı kullanarak normal veya anormal olarak sınıflandırır. Sınıflandırma temelli yaklaşımlar, bilgi tabanını oluşturan normal trafik etkinliği profiline dayanmakta ve faaliyetlerin başlangıç profilinden sapmalarını anormal olarak değerlendirmektedir [1]. Böylece sınıflandırma teknikleriyle ağ trafik desenlerinin ikili veya çoklu sınıflandırılarak kategorize edilmesi mümkün olmaktadır [3]. Destek vektör makinesi (SVM), Bayes ağları, kural tabanlı yaklaşımlar ve sinir ağları sınıflandırma tabanlı anomali tespitinde yaygın olarak kullanılan tekniklerdir.

8.2.4. Anomali Tespitinin Uygulama Alanları

Anomali tespiti günümüzde birçok alanda kullanılmaktadır. Bunlar [1,2]; izinsiz girme tespiti, sahtekârlık/dolandırıcılık tespiti, medikal anomali tespiti, endüstriyel hasar/zararların tespiti, görüntü işleme, metin verilerinde anomali tespiti, sensör ağları olarak söylenebilir.

8.2.5. Saldırı Türleri

Bu çalışma kapsamında kullanılacak veri kümesinde de yer aldığı üzere dokuz saldırı türünden [9] bahsetmek gerekmektedir. Bunlar:

- **Fuzzers:** Tam olarak Türkçe karşılığı olmamakla birlikte bulandırıcılar olarak söylenebilen bu saldırıda saldırganın bir programın, işle-

tim siteminin veya bir ağın zafiyetleri keşfetmek amacıyla rastgele ve büyük miktarlarda veri girişiyle sistemlerin çökmesine ve dolayısıyla hedef sistemin zafiyetinin keşfedilmesine olanak veren saldırı türüdür [10]. Arabellek taşması veya bellek bozulması olarak bilinen saldırılar bu türe aittir.

- **Analiz:** Port tarama, spam e-postalar veya web komut dosyaları vasıtasıyla web uygulamalarına sızma girişimlerinden oluşan çeşitli saldırıları ifade eder [10].
- **Arka kapı:** Bilgisayar üzerinde sıradan incelemeler ile bulunamayacak şekilde, normal kimlik kanıtlama süreçlerini atlatan veya kurulan bu yapıdan haberdar olan kişiye o bilgisayara uzaktan erişmeyi sağlayan yöntemler, arka kapı olarak adlandırılmaktadır [11].
- **Hizmet engelleme:** Hizmet engelleme, normal bilgi işlem ortamını bozmayı ve hizmeti kullanılamaz hâle getirmeyi hedefleyen bir ağ veya ana bilgisayarın kaynaklarına ilişkin hakların kötüye kullanılması türüdür [1]. Bu saldırının tek amacı, bir bilgisayar, sunucu veya ağın kaldırabileceğinden daha fazla yük bindirilmesi sağlanarak; sisteme yetkili kişilerin erişiminin engellenmesi ve sistemin kullanılmaz hâle getirilmesidir [11].
- **İstismar (Exploit):** Bir ana bilgisayar veya ağdaki kasıtsız veya şüphelenilmemiş bir davranıştan kaynaklanan bir aksaklık, hata veya güvenlik açığından yararlanan talimatlar dizisidir [9].
- **Jenerik:** Bir kripto-grafik ilkeye karşı genel bir saldırıdır. Söz konusu kripto yaklaşımın nasıl uygulandığının detaylarından bağımsız olarak çalıştırılabilen saldırıdır. Örneğin; K bit anahtarlı bir şifre metni olduğu varsayıldığında, saldırgan k bitlerini, yani 2K kombinasyonlarını kullanarak mümkün olan her kombinasyonu dener -buna kaba kuvvet saldırısı da denir- ve metnin şifresini çözmeye çalışır [10].
- **Keşif (Reconnaissance):** Bir bilgisayar ağı hakkında güvenlik denetimlerinden kaçınmak için bilgi toplayan bir saldırı olarak tanımlanabilir [9]. Ayrıca keşif saldırıları, bir ağa bağlı makinelerin türleri ve sayıları hakkında bilgi toplamanın oldukça yaygın yoludur ve yüklü olan yazılım türlerini ve/veya kullanılan uygulamaları belirlemek için bir ana makineye saldırılabilir [1].

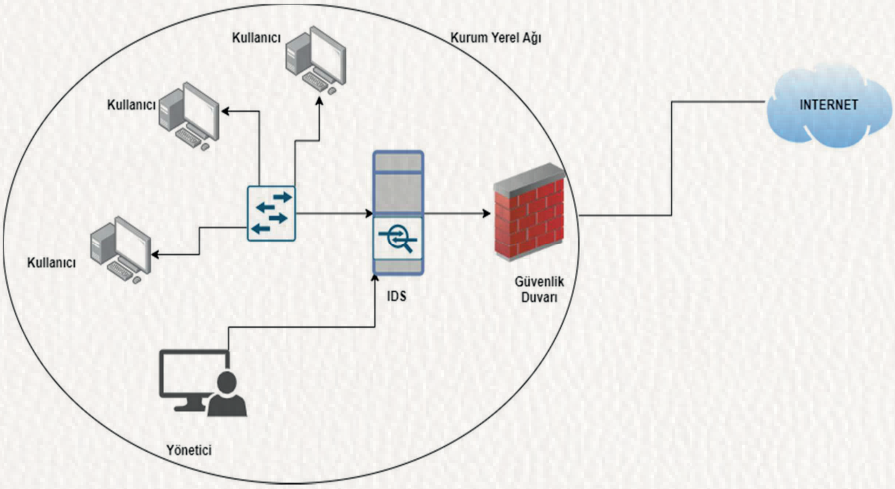
- **Kabuk kodu (Shellcode):** Saldırganın hedef makineye sızarak kabuk (shell) üzerinden kod parçacıklarını çalıştırıp sistemi ele geçirmesini sağlayan saldırıdır. Kabuk kodları yerel (local) veya uzak (remote) bir şekilde çalıştırılabilirler. Bu bağlamda uzaktan çalıştırılan bu kodlarla R2U (Remote to user) saldırıları gerçekleştirilebilir.
- **Solucan (Worm):** Genellikle ağ bağlantısı, indirilen bir dosya yoluyla, hedef bilgisayardaki bir açıklık veya sosyal mühendislik yöntemleriyle sisteme sızmaya çalışan ve sisteme girdikten sonra ise ağ veya internet bağlantısı üzerinden kendisinin birden fazla işlevsel kopyasını yaparak yayılan, ağdaki yeterince korunmayan tüm bilgisayarları ve sunucuları etkileyen saldırı türüdür [12].

Söz konusu bu saldırı türleri dışında kod istismarı, dolaylı veya doğrudan erişim saldırıları, sosyal mühendislik gibi aktif ve pasif olmak üzere iki temel grupta incelenen birçok saldırı türü vardır fakat bunlar bu çalışma kapsamında ele alınmayacaktır.

8.2.6. Ağ Saldırı Tespit Sistemleri

Saldırı tespit sistemlerinin (IDS-Intrusion Detection System) bir türü olan ağ saldırı tespit sistemleri (NIDS-Network Intrusion Detection System) kısaca ağlara karşı yapılan kötü niyetli eylemlerin veya politika ihlallerinin izlenmesini ve tespitini yapan sistemler olarak adlandırılır. Bir NIDS, sensörler aracılığıyla belirli ağ bölümündeki ağ trafiğini yakalayarak şüpheli olayları tanımak için uygulamaların ve protokollerin etkinliklerini analiz eder [13]. Ağ saldırı tespit sistemlerinin saldırılara karşı herhangi bir aksiyon alma özelliği yoktur. Bu sistemlerin temel görevi kötü niyetli aktiviteleri tespit etmek ve saldırı türünü raporlamaktır. İdeal bir ağ saldırı tespit sisteminin gelen ve giden tüm trafiği taraması gerekmektedir. Ancak bu durum ağ trafiğinin hızını azaltan tıkanıklıklara sebep olabilmektedir. Bu sistemlerin çevrim içi ve çevrim dışı olmak üzere iki tasarım tipi vardır. Çevrim içi ağ tabanlı saldırı tespit sistemi, ağ ile gerçek zamanlı ilgilenir ve bir saldırı olup olmadığına karar vermek için Ethernet paketlerini analiz ederek bazı kurallar uygular [14]. Çevrim dışı ağ tabanlı saldırı tespit sistemi, depolanan verileri ele alır ve bir saldırı olup olmadığına karar vermek için bazı işlemlerden geçirir [14]. Saldırı tespit sistemleri, saldırıları tespit

etmek için imza tabanlı algılama ve anomali tabanlı algılama olmak üzere iki tip mekanizmayı benimsemiştir. İmza tabanlı sistemlerde bilinen izinsiz giriş faaliyetleri tespit edilir yani saldırının karakteristiğinde bulunan birtakım modeller aranarak saldırılar tespit edilmeye çalışılır [3]. Özellikle anti virüs teknolojilerinde kullanılan bu yaklaşımda bilinen bir saldırının tespiti kolayca yapılabilirken, modeli olmayan yeni saldırılara karşı başarı sağlanamamaktadır. Anomali tabanlı yaklaşımda ise olağandışı yani önceden bilinmeyen izinsiz giriş faaliyetleri tespit edilmeye çalışılır [3]. Burada temel amaç güvenilir bir öğrenme modeli oluşturup yeni gelen modelleri bununla karşılaştırmaktır. Bilinmeyen yeni saldırılara karşı daha başarılı olan bu yöntemde bilinmeyen fakat yasal olan eylemler için yanlış alarm üretilebilmektedir. Şekil 8.2'de bir ağ saldırı tespit sisteminin ağda nasıl konumlandırılabileceğinin bir örneği görülmektedir.



Şekil 8.2. Saldırı tespit sisteminin ağ üzerinde konumlandırılması

8.2.7. Ağ Anomali Tespitinde Karşılaşılan Zorluklar

Günümüzde anomali tespitinde birçok teknik kullanılmaktadır. Teknolojinin gelişimiyle birlikte anomali tespitindeki kabiliyetlerimiz ne kadar gelişmiş olsa da anomali tespiti noktasında hâlâ birtakım zorluklar var olmaya devam etmektedir. Bunlar [1-3, 15];

- Evrensel olarak uygulanabilir anomali tespit tekniğinin eksikliği. Örneğin, kablolu bir ağdaki izinsiz giriş algılama tekniği, kablosuz bir ağda çok az kullanılabilir,
- Verilerin gürültü içermesi bu gürültülerin gerçek anomali olarak algılanmasına sebep olması,
- Veri setlerinde sınıf dengesizliklerinin olması,
- Kategorik verilerde bir örüntü belirlemenin veya bir mesafe ölçmenin zor olması sebebiyle anomali saptama yöntemlerinin kategorik verilerde başarı oranının düşük olması,
- Gerçek hayat problemlerinde ele alınan veri setlerinin çok büyük miktarda olmasının, çok fazla gözlem ve kategorik veri içermesinin zaman karmaşıklığının artmasına yol açması,
- Ağ anomali tespiti için kullanılabilecek herkes tarafından erişilebilen etiketlenmiş veri seti eksikliği,
- Normal aktivitelerin sürekli olarak evrim geçiriyor olması şu an ki sistemlerin ileride güncelliğini yitirmesine sebep olacak olması,
- Olası her normal davranışı tanımlamanın oldukça zor olması,
- Normal ve anormal aktiviteler arasında kesin bir sınırın olmaması ve
- Anomalilere sebep olan kötücül eylemlerin kendilerini normal gibi gösterebilme yeteneğini kazanması

şeklinde ifade edilebilir.

8.3. UYGULAMADA KULLANILAN ARAÇ VE YÖNTEMLER

8.3.1. Araçlar

Ağ anomali tespiti için karşılaştırılacak algoritmaların uygulanmasında ve elimizde bulunan veri kümesi için karar verilen en uygun algoritma çerçevesinde uygulamayı geliştirirken kullanılan araç ve teknikler kısaca maddeler hâlinde aşağıda olduğu gibidir.

- **İşletim sistemi:** Bu uygulama, x64 tabanlı 2.40 GHz hızında bir işlemci ve 8 GB RAM'e sahip bir Windows işletim sistemi üzerinde gerçekleştirilmiştir.

- **Programlama dili:** Uygulama geliştirilirken programlama dili olarak Python 3.6.7 sürümü kullanılmıştır.
- **Geliştirme ortamı:** Anaconda dağıtımı üzerinden Jupyter Notebook geliştirme ortamı kullanılmıştır.
- **Kütüphaneler:** Bu uygulamanın geliştirilmesinde;
  - → **Pandas:** Veri kümesinin okunması, düzenlenmesi, tablolar hâlinde gösterilmesinde kullanılmıştır.
  - → **Scikit-learn:** Python makine öğrenmesi kütüphanesidir. Uygulama kapsamındaki veri kümesinin ölçeklendirilmesinde ve sınıflandırma algoritmalarının uygulanmasında kullanılmıştır.
  - → **Seaborn, Matplotlib:** Algoritmaların uygulanması sonucunda oluşturulan kümelerin grafiksel gösteriminde kullanılmıştır.

8.3.2. Sınıflandırma Algoritmaları

Bu proje kapsamında ağ saldırılarının tespit edilebilesi amacıyla verilerin normal ve anormal olarak düzgün bir şekilde ayrıştırılabilmesi amacıyla en uygun sınıflama yapan algoritmaya karar vermek için Karar Ağacı, Gradyan Arttıma Makineleri (Gradient Boosting Machines), XGBoost, LightGBM, CatBoost, En Yakın Komşu (KNN), Lineer Regresyon, Naive Bayes ve Destek Vektör Makinesi (SVM) algoritmaları karşılaştırılmıştır. Sınıflandırma algoritmaları veri kümesindeki verilerin sınıf etiketlerinin bilindiği durumlarda kullanılan danışmanlı öğrenme algoritmalarıdır. Sınıflandırma işlemi sırasında her bir gözleme bir sınıf atması yapılır. Bu algoritmaların tanımı ve çalışma şekilleri, sınıflandırma için gerekli parametreleri aşağıda detaylı olarak incelenmiştir.

i. Lineer regresyon algoritması

Doğrusal (linear) modeller pratikte yaygın olarak kullanılan yaklaşımlardır. Doğrusal modeller, girdi özelliklerinin doğrusal bir işlevini kullanarak bir tahmin yaparlar [16]. Türkçeye doğrusal regresyon olarak çevrilebilen bu algoritma bir değişkenin değerini (y) belirli bir özellik kümesine (x) göre tahmin etmek için kullanılır [7]. Lineer modeller için genel tahmin denklemi Eşitlik (8.1)'de olduğu gibidir [14].

$$\hat{y} = w[0] * x[0] + w[1] * x[1] + ... + w[p] * x[p] + b \quad (8.1)$$

Burada doğrusal regresyon, eğitim setindeki tahminler ve gerçek regresyon hedefleri (y) arasındaki ortalama kare hatasını en aza indiren w ve b parametrelerini bulmaya çalışır. Burada nokta şeklinde görülenler eğitim veri setinin iki boyutlu uzayda dağılımını temsil etmektedir. Doğrusal regresyonda temel amaç eğitim setindeki bu noktaların tamamına en yakın geçen doğruyu çizmektir. Bu doğru denklemindeki katsayılarının bulunması ve çok sayıdaki karmaşık hesaplama ve ölçümlere dayalı verinin basit bir doğruya indirgenmesi işlemi doğrusal regresyon tarafından gerçekleştirilmiş olur. Doğrusal regresyonun hiçbir parametresi yoktur, bu bir fayda olarak düşünülebilir ancak model karmaşıklığını kontrol etmek bu sebeple mümkün olmamaktadır [16].

ii. K-en yakın komşu algoritması

K-en yakın komşu algoritması tartışmasız en basit danışmanlı makine öğrenmesi algoritmasıdır ve modelin oluşturulması sadece eğitim veri kümesinin saklanması ile gerçekleştirilir, yeni bir veri noktası için bir tahmin yapmak üzere algoritma, eğitim veri kümesindeki en yakın veri noktalarını yani "en yakın komşularını" bulur [16].

iii. Naive Bayes algoritması

Naive Bayes sınıflandırıcılar, doğrusal modellere oldukça benzeyen bir sınıflandırıcı ailesidir, eğitimde daha da hızlı olma eğilimindedirler ancak Naive Bayes modellerinin genellikle Logistik Regresyon ve LinearSVM gibi doğrusal sınıflandırıcılardan biraz daha kötü olan genelleme performansı sağlamaktadır [16]. Naive Bayes modellerinin bu kadar verimli olmasının nedeni, her bir özelliğe ayrı ayrı bakarak parametreleri öğrenmeleri ve her özellikten sınıf başına basit istatistikler toplamalarıdır. Bunu yaparken Eşitlik (8.2)'de verilen koşullu olasılık değerlerini hesaplarlar.

$$P(A \mid B) = P(A)\, P(B \mid A) / P(B) \quad (8.2)$$

Burada P (A|B) B olayı gerçekleştiğinde A olayının gerçekleşme olasılığı, P (A) A olayının gerçekleşme olasılığı, P (B) B olayının gerçekleşme olasılığı, P (B|A) A olayı gerçekleştiğinde B olayının gerçekleşme olasılığı olarak karşımıza çıkmaktadır.

iv. Destek Vektör Makinesi (SVM) algoritması

Destek Vektör Makinesi'nin temel prensibi, pozitif ve negatif sınıflar arasındaki ayrım payını en üst düzeye çıkaran bir hiper düzlem elde etmektir [8]. SVM'nin ilginç bir özelliği, istatistiksel öğrenme teorisine dayanan yapı riskini en aza indirme prensibinin yaklaşık bir uygulaması olmasıdır [1]. SVM bir danışmanlı öğrenme makine öğrenmesi çeşididir ve sınıflandırma yapabilmek için etiketlenmiş veriye ihtiyaç duymaktadır. Radyal temel işlevi (RBF) çekirdeği gibi çekirdekler, karmaşık bölgeleri öğrenmek için kullanılabilir. Her test örneği için, model test örneğinin öğrenilen bölge içinde olup olmadığını belirler ve eğer bir test örneği öğrenilen bölge içindeyse, normal, diğer durumda anormal olarak bildirilir [2].

v. Karar ağacı algoritması

Karar ağacı, her iç düğümün (yapraksız düğüm) bir öznitelik üzerinde bir testi temsil ettiği, her dalın testin bir sonucunu temsil ettiği ve her yaprak düğümünün (veya terminal düğümünün) bir sınıf etiketi içerdiği akış şeması benzeri bir ağaç yapısıdır [17]. En üstteki düğüm bölünmenin ilk başladığı kök düğüm (root node) olarak adlandırılır. Burada bilgisayar alım durumu üzerinden sınıflandırma yapılması konseptinde oluşturulan bir ağaç yapısı çizilmiştir. Örneğin orta yaşlı birisinin bilgisayar alan sınıfında olduğu bunun yanı sıra genç ve öğrenci olan birisinin bilgisayar almayan sınıfta olduğu ağaç yapısından görülebilmektedir.

vi. Gradyan arttırma makineleri algoritması

Gradyanla güçlendirilmiş regresyon ağacı veya diğer bir deyişle gradyanla güçlendirilmiş makineler, daha güçlü bir model oluşturmak için birden fazla karar ağacını birleştiren bir kolektif (ensemble) yöntemdir [16]. Bu yöntem hem regresyon hem de sınıflandırma için kullanılabilmektedir. Gradyan artırma, her ağacın bir öncekinin hatalarını düzeltmeye çalıştığı seri bir şekilde ağaçlar oluşturarak çalışmaktadır ve varsayılan olarak, gradyan destekli regresyon ağaçlarında herhangi bir rastgele sıralama yoktur; bunun yerine güçlü ön budama (pre-pruning) kullanılır [16]. Derinliği az olan ağaçlardan oluşturularak hafıza kullanımını aza indirip tahminleri daha hızlı yapmaya

çalışır. Bahsi geçen bu küçük ağaçlar veriden en iyi tahmin yapılan kısımları temsil ederler ve bunların her biri tekrarlamalı olarak ana yapıya eklenerek performansı arttırmaya çalışır. Bu durum gradyan destekli makinelerin temel amacını oluşturmaktadır.

vii. XGBoost algoritması

XGBoost, karar-ağacı (decision-tree) temelli ve eğim-arttırmalı (gradient-boosting) bir makine öğrenmesi algoritmasıdır. Veri bilimcileri tarafından yaygın olarak kullanılan ve birçok problem üzerinde son teknoloji sonuçlar veren uçtan uca ölçeklenebilir bir ağaç güçlendirme sistemidir [18]. XGBoost, birçok veri bilimi problemini hızlı ve doğru bir şekilde çözen paralel bir ağaç güçlendirmesi (GBDT, GBM olarak da bilinir) sağlar [19]. XGBoost, ilk olarak Washington Üniversitesinde iki araştırmacı olan Tianqi Chen ve Carlos Guestrin tarafından SIGKDD 2016 konferansında makale olarak sunulmuştur. XGBoost'un GBM'e göre, hem sistem (donanım ve yazılım) optimizasyonu hem de algoritmik geliştirmeleri bu algoritmanın sadece akademik çalışmalarda değil birçok platformda veri bilimi yarışmalarında kullanılmasını sağlamıştır.

viii. LightGBM algoritması

LightGBM'de ağaç tabanlı öğrenme algoritmaları kullanan bir eğim arttırmalı yaklaşımdır [20]. Hızlı ve verimli bir şekilde modeli eğitmesi, düşük hafıza kullanımı, daha iyi doğruluk oranı, paralel ve GPU kullanarak öğrenme desteği, büyük ölçekli verileri işleyebilme yeteneği avantajları olarak bahsedilmektedir. Bu algoritmanın diğer ağaç tabanlı algoritmalardan farkı dikey olarak büyümesidir. Açık bir şekilde sunulan birçok veri seti üzerinde yapılan deneyler sonucunda LightGBM'in, geleneksel GBDT'nin eğitim sürecini neredeyse aynı doğruluğa ulaşırken 20 kata kadar hızlandırdığı görülmüştür [21].

ix. CatBoost algoritması

Bu algoritmada XGBoost ve LightGBM gibi karar-ağacı (decision-tree) temelli ve eğim-arttırmalı (gradient-boosting) bir açık kaynak kodlu ma-

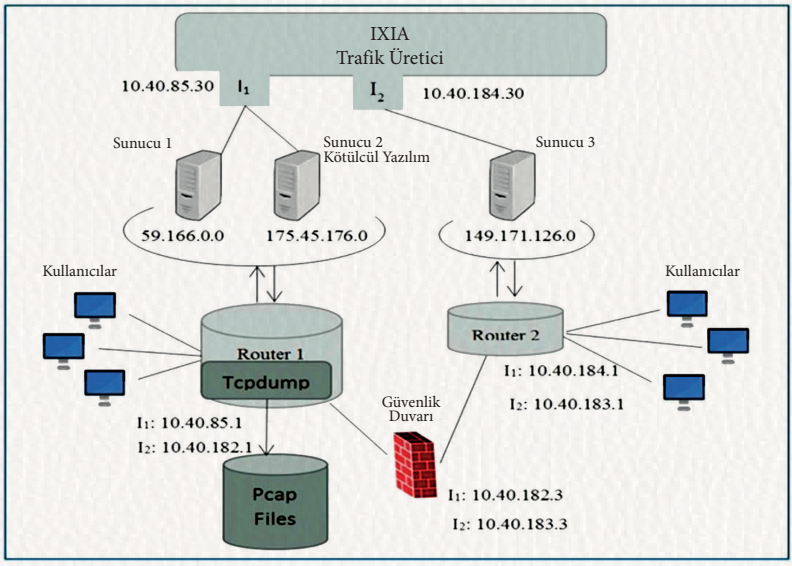
kine öğrenmesi algoritmasıdır. Yandex çalışanları tarafından geliştirilmiştir. CatBoost'ta sunulan kritik algoritmik ilerlemeler, sıralı güçlendirmenin uygulanması, klasik algoritmaya permütasyon odaklı bir alternatif sunması ve kategorik özellikleri işlemek için yenilikçi bir algoritma olmasıdır [22]. Kategorik değişkenleri direkt olarak işleyebiliyor olması beraberinde birçok kolaylık getirmiştir.

8.4. UYGULAMANIN GERÇEKLEŞTİRİLMESİ

8.4.1. Veri Setinin İncelenmesi

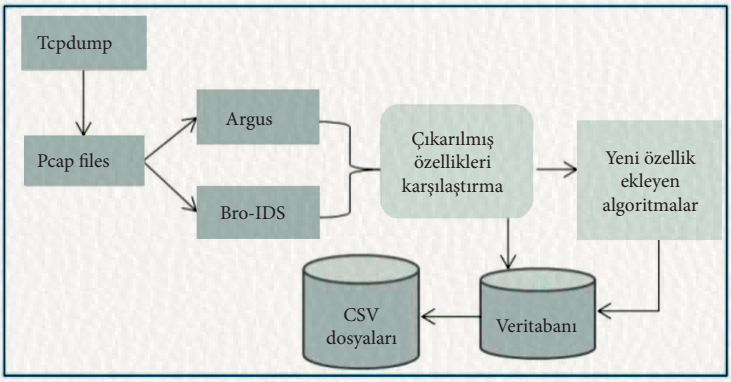
Makine öğrenmesi algoritmaları ile anomali tabanlı saldırı tespiti ve karşılaştırmalı analizi kapsamında gerçekleştiren bu çalışmada Kaggle[1] platformundan elde edilen ve 175341 satırdan oluşan bir ağ trafik veri seti kullanılmıştır. Ham ağ paketleri verisinden oluşan UNSW-NB15 adlı veri setinin, günümüze şartlarına uygun gerçek normal faaliyetlerin ve sentetik saldırı davranışlarının bir melezini oluşturmak için Avustralya Siber Güvenlik Merkezi'nin (ACCS) Cyber Range Lab isimli laboratuvarda IXIA PerfectStorm aracı tarafından oluşturulmuştur. Söz konusu ham ağ trafik verilerinin toplanmasında TCPdump aracı kullanılmıştır. IXIA aracı üzerinden simüle edilen anormal trafik Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode ve Worms olmak üzere dokuz tip saldırıyı içermektedir ve bu saldırılar ortak güvenlik açıkları yayınlandığı CVE[2] sitesi üzerinden sürekli güncellenen saldırı tipleridir [23]. Toplanan bu ağ trafik verilerinin normal ve anormal olarak 49 özellik (features) üzerinden doğru bir şekilde etiketlendirilmesinde Argus, Bro-IDS adlı ağ saldırı tespit sistemi araçları kullanılmıştır. Veri setinin oluşturulmasında kurulan ortam ve araçlar Şekil 8.3'te gösterilmektedir.

1 https://www.kaggle.com/mrwellsdavid/unsw-nb15
2 https://cve.mitre.org/



Şekil 8.3. Veri setinin oluşturulma ve sınama ortamı [24]

Veri seti oluşturulurken PCAP dosyalarından CSV dosyalarına dönüşüm de dâhil olmak üzere 49 özelliğe sahip UNSW-NB15'in son şeklinin oluşturulmasında yer alan tüm mimari çerçeve ise Şekil 8.4'te gösterilmektedir.



Şekil 8.4. UNSW-NB15 oluşturulurken kurulan mimari çerçeve [23]

Söz konusu veri setinden çıkarılan 49 özellik, bu özelliklerin veri tipi ve tanımları Tablo 8.1'de detaylı bir şekilde verilmiştir. Ek olarak bu özellikler akış, temel, içerik, zaman (time) ve ek (additional) özellikler olmak üzere beş grupta ele alınmıştır [24].

Tablo 8.1. Veri setinde bulunan özelliklerin isim, tür ve tanımları

No	İsim	Tür	Tanım
1	srcip	Nominal	Kaynak IP adresi
2	sport	Integer	Kaynak port numarası
3	dstip	Nominal	Hedef IP adresi
4	dsport	Integer	Hedef port numarası
5	proto	Nominal	İletim protokolü
6	state	Nominal	Durum ve bağlı olduğu protokol (Örn: ACC, CLO, else(-))
7	dur	Float	Toplam süre kaydı
8	sbytes	Integer	Kaynaktan hedefe giden bayt
9	dbytes	Integer	Hedeften kaynağa giden bayt
10	sttl	Integer	Kaynaktan hedefe atlama sınırı (time to live)
11	dttl	Integer	Hedeften kaynağa atlama sınırı (time to live)
12	sloss	Integer	Atılan veya tekrar gönderilen kaynak paketleri
13	dloss	Integer	Atılan veya tekrar gönderilen hedef paketleri
14	service	Nominal	http, ftp, ssh, dns…, else (-)
15	sload	Float	Kaynağın saniyedeki bit sayısı
16	dload	Float	Hedefin saniyedeki bit sayısı
17	spkts	Integer	Kaynaktan hedefe giden paket sayısı
18	dpkts	Integer	Hedeften kaynağa gelen paket sayısı
19	swin	Integer	Kaynak TCP pencere reklamı/duyurusu
20	dwin	Integer	Hedef TCP pencere reklamı/duyurusu
21	stcpb	Integer	Kaynak TCP sıra (sequence) numarası
22	dtcpb	Integer	Hedef TCP sıra numarası
23	smeanz	Integer	Kaynak tarafından iletilen akış paketi boyutunun ortalaması
24	dmeanz	Integer	Hedef tarafından iletilen akış paketi boyutunun ortalaması
25	trans_depth	Integer	http istek / yanıt işleminin bağlantı derinliği
26	res_bdy_len	Integer	Sunucunun http hizmetinden aktarılan verilerin içerik boyutu
27	sjit	Float	Kaynak jitter (mSec)
28	djit	Float	Hedef jitter (mSec)
29	stime	Timestamp	İlk kayıt zamanı
30	ltime	Timestamp	Son kayıt zamanı
31	sintpkt	Float	Kaynak paketler arası varış zamanı (mSec)
32	dintpkt	Float	Hedef paketler arası varış zamanı (mSec)
33	tcprtt	Float	TCP'nin "synack" ve "ackdat" toplamı
34	synack	Float	TCP'nin SYN ve SYN_ACK paketleri arasındaki süre
35	ackdat	Float	TCP'nin SYN_ACK ve ACK paketleri arasındaki süre
36	is_sm_ips_ports	Binary	Kaynak hedef IP adresleri eşitse ve port numaraları eşitse, bu değişken 1 değerini alır diğer durumda 0
37	ct_state_ttl	Integer	Kaynak/hedef ttl' i için özel aralık değerleri içeren her bir durum sayısı

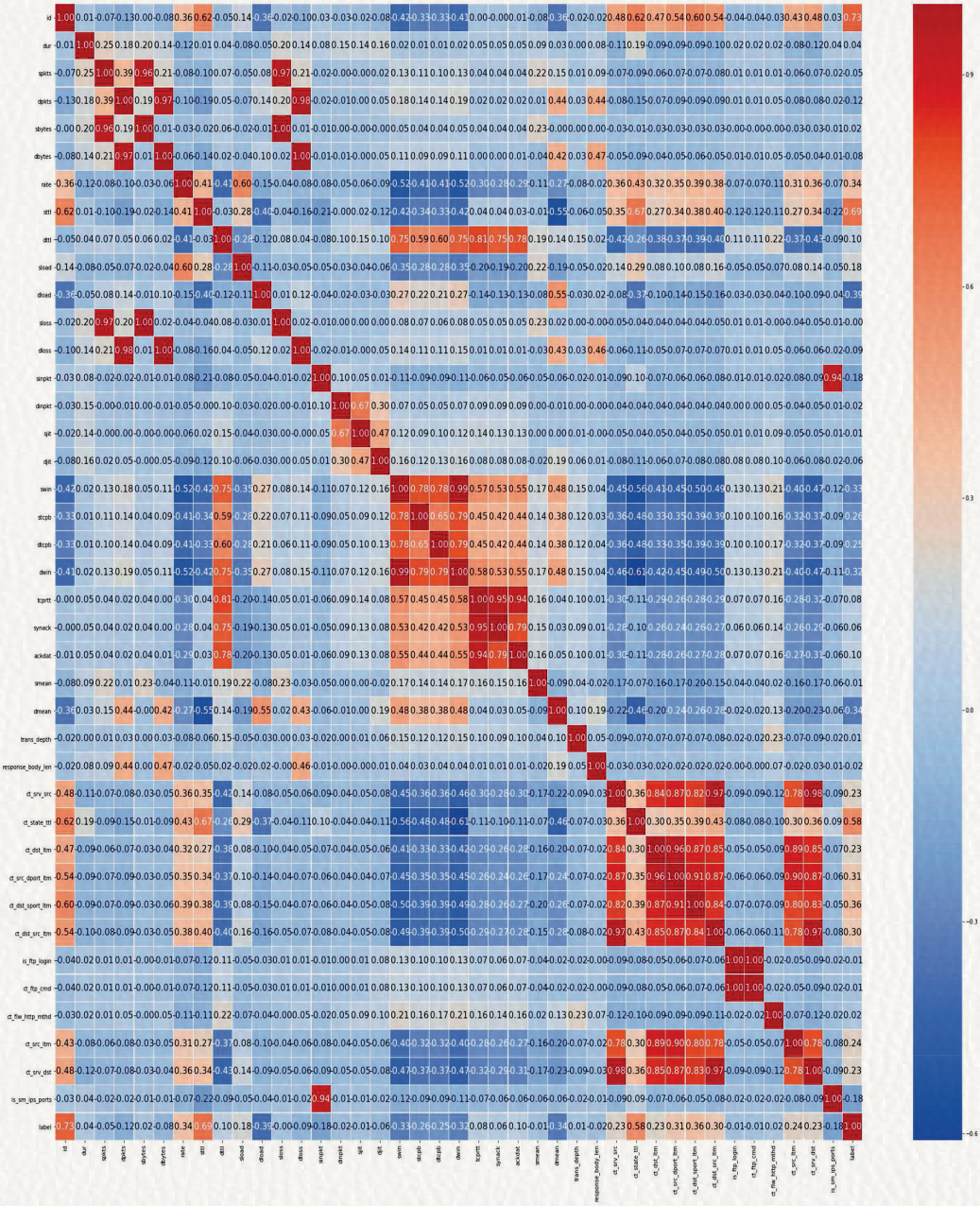
Tablo 8.1. (Devam) Veri setinde bulunan özelliklerin isim, tür ve tanımları

38	ct_flw_http_mthd	Integer	http get/post metotlarına sahip akış sayısı
39	is_ftp_login	Binary	Eğer ftp oturumu kullanıcı ve parola ile erişilirse 1, değilse 0
40	ct_ftp_cmd	Integer	Ftp oturumunda komutu olan akışların sayısı
41	ct_srv_src	Integer	Son zamana göre 100 bağlantı içinde aynı servis ve hedef adresine sahip bağlantı sayısı
42	ct_srv_dst	Integer	Son zamana göre 100 bağlantı içinde aynı servis ve kaynak adresine sahip bağlantı sayısı
43	ct_dst_ltm	Integer	Son bağlantı zamanına göre 100 bağlantı içinde aynı hedef adresine sahip bağlantı sayısı
44	ct_src_ ltm	Integer	Son bağlantı zamanına göre 100 bağlantı içinde aynı kaynak adresine sahip bağlantı sayısı
45	ct_src_dport_ltm	Integer	Son zamana göre 100 bağlantıda aynı kaynak adres ve hedef portun bağlantı sayısı
46	ct_dst_sport_ltm	Integer	Son zamana göre 100 bağlantıda aynı hedef adres ve kaynak portun bağlantı sayısı
47	ct_dst_src_ltm	Integer	Son zamana göre 100 bağlantıda aynı kaynağın ve hedef adresin bağlantı sayısı
48	attack_cat	Nominal	Her bir saldırı kategorisinin ismi.
49	Label	Binary	Normal için 0, saldırı için 1 olan kayıtlar yani sınıf etiketi

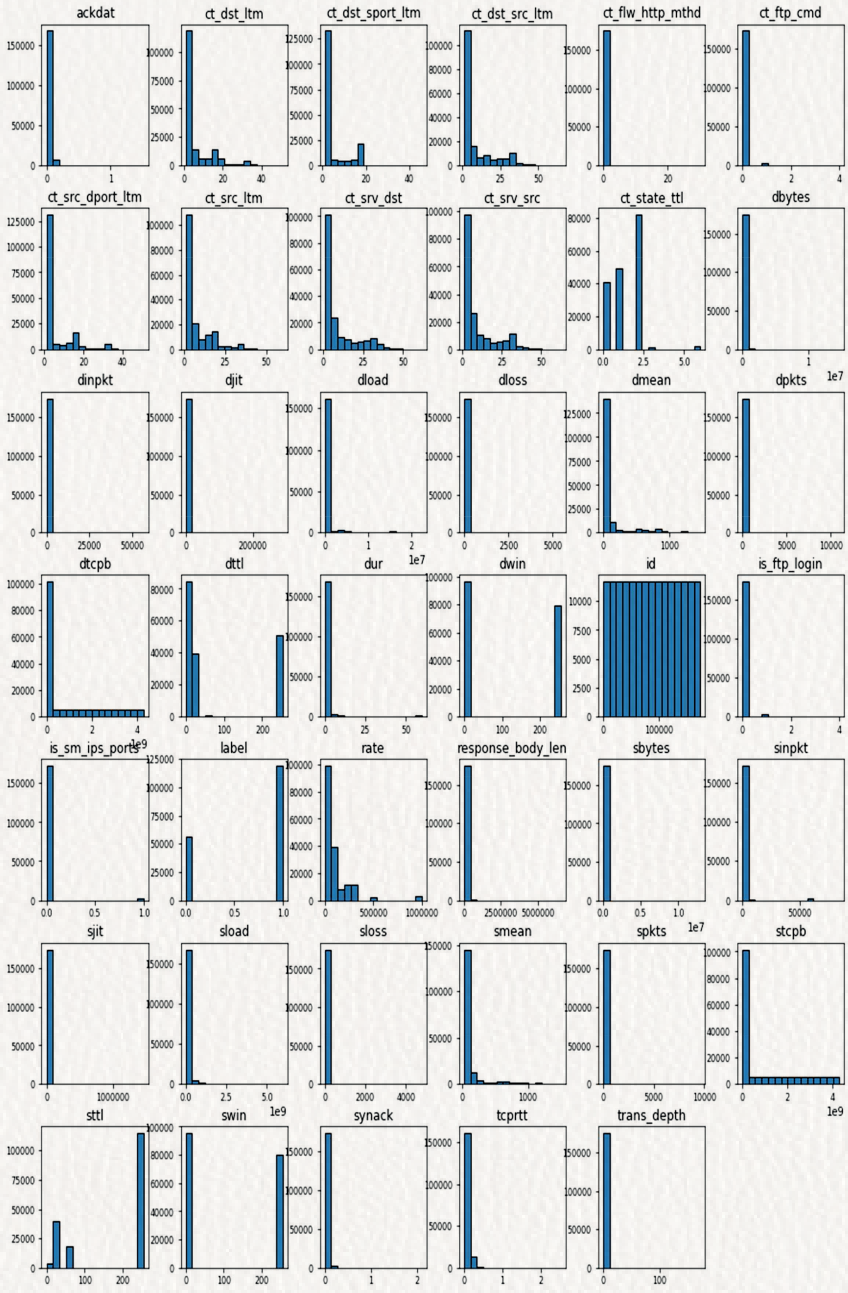
Tablo 8.1'de verilen 1-5 arası özellikler akış, 6-18 arası özellikler temel, 19-26 arası özellikler içerik, 27-35 arası özellikler zaman, 36-40 arası özellikler ek özelliklerden genel amaçlı olanları, 41-47 arası özellikler ek özelliklerden bağlantı ile ilgili olanları, 48-49 ise etiketlenmiş özellikleri temsil etmektedir.

8.4.2. Veri Setinin Görselleştirilme İşlemleri

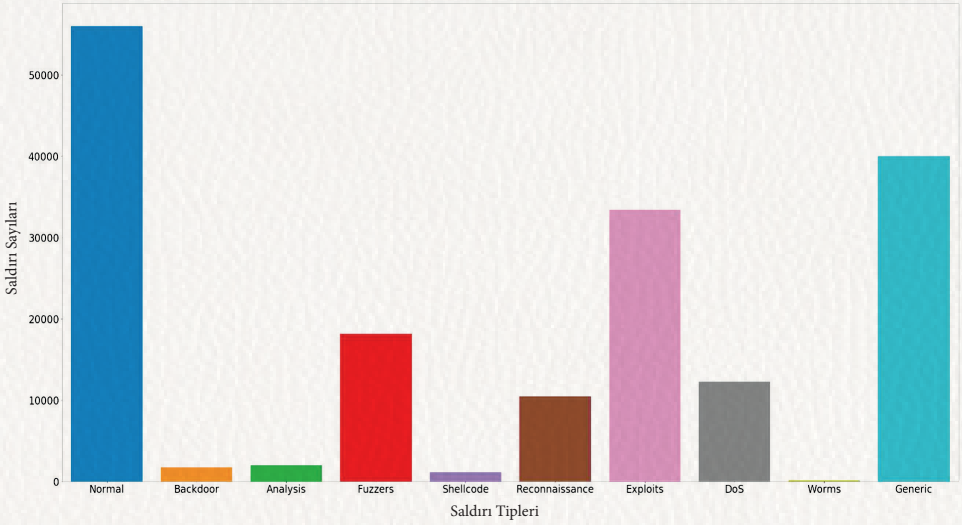
Veri setindeki özelliklerin daha iyi anlaşılıp yorumlanabilmesi açısından bu çalışma kapsamında korelasyon matrisi ve veri dağılımlarının sütun grafiklerini içeren birtakım veri görselleştirilmeleri yapılmıştır. Şekil 8.5'te özellikler arasındaki ilişkileri -0.7–1.0 aralığında puanlayarak gösteren korelasyon matrisi görülmektedir. Şekil 8.6'da veri setindeki sayısal değerlerin dağılım grafikleri görülmektedir. Şekil 8.7'de veri setinde bulunan saldırı tiplerinin dağılımı ve son olarak Şekil 8.8'de ise normal ve anormal olarak sınıflandırılan verilerin dağılımı görülmektedir.



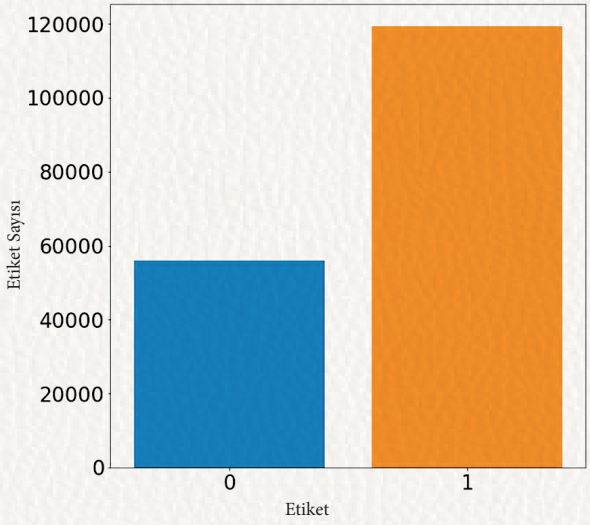
Şekil 8.5. Veri seti özellik ısı haritası korelasyon matrisi



Şekil 8.6. Veri setindeki sayısal özelliklerin dağılım grafikleri



Şekil 8.7. Saldırı tiplerinin dağılım grafiği



Şekil 8.8. Normal (0) ve anormal (1) etiketine sahip verilerin dağılım grafiği

Yukarıdaki şekillerden yola çıkılarak veri setinde bulunan örneklerin düzgün dağılım göstermediği tespit edilmiştir. Bu durum sınıflandırma algoritmalarının performansını etkileyebilecek derecede öneme sahiptir.

8.4.3. Veri Seti Üzerinde Uygulanan İşlemler

Bu uygulama kapsamında veri setine uygulanacak algoritmaların en doğru sonuçları verebilmesi için veri seti üzerinde birtakım işlemlerin yapılması gerekmektedir. Bu amaçla veri seti öncelikle Python'ın desteklediği Pandas kütüphanesi verilerin daha okunaklı bir şekilde görselleştirilmesi ve gereksiz satır ve sütunların temizlenmesi için kullanılmıştır. Şekil 8.9'da veri setinin bir kısmının herhangi satır sütun işlemi yapılmadan önceki hâli görülmektedir.

Out[41]:

	id	dur	proto	service	state	spkts	dpkts	sbytes	dbytes	rate	...	ct_dst_sport_ltm	ct_dst_src_ltm	is_ftp_login	c
0	1	0.000011	udp	-	INT	2	0	496	0	90909.093750	...	1	2	0	
1	2	0.000008	udp	-	INT	2	0	1762	0	125000.000000	...	1	2	0	
2	3	0.000005	udp	-	INT	2	0	1068	0	200000.000000	...	1	3	0	
3	4	0.000006	udp	-	INT	2	0	900	0	166666.656250	...	1	3	0	
4	5	0.000010	udp	-	INT	2	0	2126	0	100000.000000	...	1	3	0	
5	6	0.000003	udp	-	INT	2	0	784	0	333333.312500	...	1	2	0	
6	7	0.000006	udp	-	INT	2	0	1960	0	166666.656250	...	1	2	0	
7	8	0.000028	udp	-	INT	2	0	1384	0	35714.285156	...	1	3	0	
8	9	0.000000	arp	-	INT	1	0	46	0	0.000000	...	2	2	0	
9	10	0.000000	arp	-	INT	1	0	46	0	0.000000	...	2	2	0	

10 rows × 45 columns

Şekil 8.9. Veri seti görüntüsü

Daha sonra veri setinde bulunan özelliklerin istatistiksel özelliklerine bakılmıştır. Herhangi bir null değer olup olmadığı kontrol edilmiştir. Varsa bunlar temizlenmiştir. Çünkü bu değerler algoritmaların başarı oranlarını etkilemektedir. Algoritmaları eğitirken işimize yaramayacak olan id ve attack_cat sütun değerleri atılmıştır. Son olarak state, service ve proto sütunlarında yer alan kategorik veriler algoritmaların işleyebileceği forma dönüştürme işlemi one-hot-encoding yöntemiyle gerçekleştirilmiştir. Bu işleminin doğası gereği işlem sonrasında veri setinin boyutu artmış ve 194 sütuna çıkmıştır. Tüm işlemler sonrası veri setinin son durumu Şekil 8.10'da görülmektedir.

dbytes	rate	sttl	dttl	sload	dload	...	service_snmp	service_ssh	service_ssl	state_ACC	state_CLO	state_CON	state_FIN
3740	81.226723	31	29	1.781109e+04	2.271873e+04	...	0	0	0	0	0	0	1
0	142857.140625	254	0	6.514286e+07	0.000000e+00	...	0	0	0	0	0	0	0
0	100000.000000	254	0	4.560000e+07	0.000000e+00	...	0	0	0	0	0	0	0
0	0.000000	0	0	0.000000e+00	0.000000e+00	...	0	0	0	0	0	0	0
268	78.948196	254	252	5.532690e+04	9.431678e+03	...	0	0	0	0	0	0	1
...	...	...	...	...	...	...	...	...	...	...	...	...	...
642	23.087734	254	252	5.312026e+03	4.351576e+03	...	0	0	0	0	0	0	1
0	0.348294	254	0	1.253859e+02	0.000000e+00	...	0	0	0	0	0	0	0
698	59.009911	254	252	4.220200e+05	4.122826e+03	...	0	0	0	0	0	0	1
1152	14.899015	62	252	5.076182e+03	7.067392e+03	...	0	0	0	0	0	0	1
79882	1158.875610	31	29	2.635928e+05	4.331260e+06	...	0	0	0	0	0	0	1

Şekil 8.10. Veri seti son durum

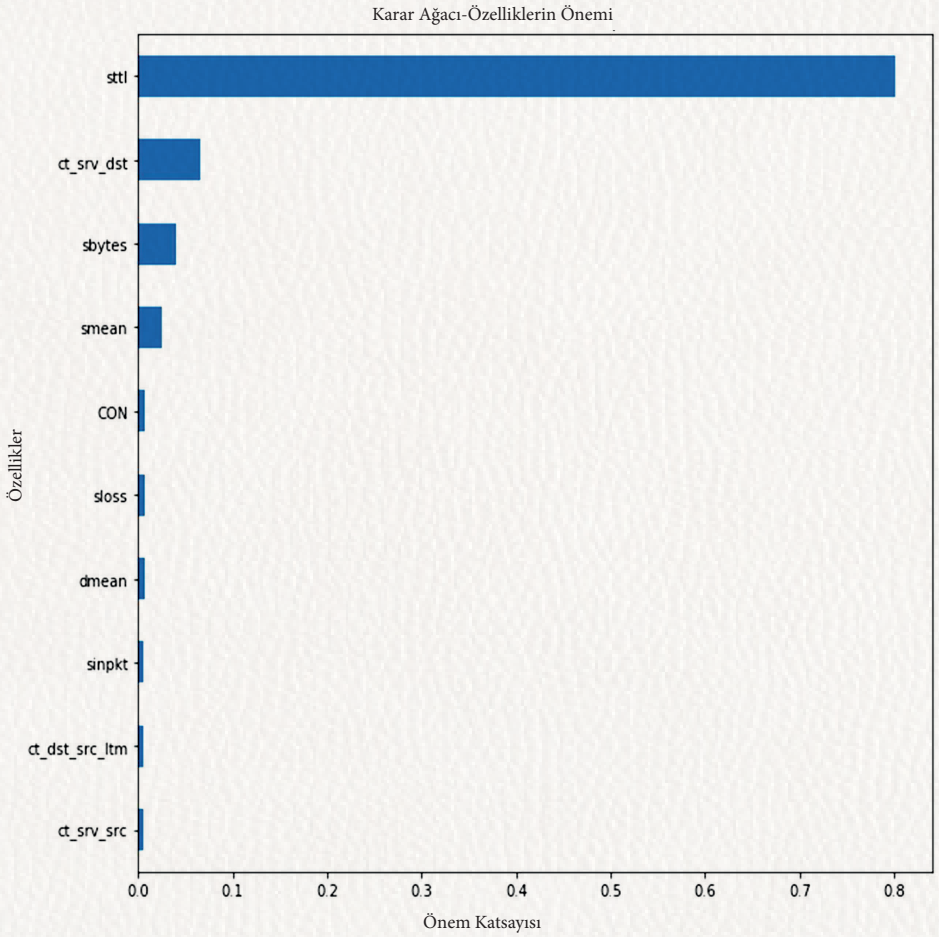
Son olarak doğrusal sınıflandırma modellerinin başarı oranının arttırılması için de veri seti üzerinde standart ölçekleme ve veri setinin boyutunun küçültülmesi içinde PCA uygulanmıştır. PCA uygulanırken veri dağılımının %95 oranında korunması dikkate alınmıştır. Bu sebeple boyut azaltma işlemi sonrası sütun sayısı 194'ten 153'e düşmüştür. Veri dağılımının korunması oranı düştükçe boyut azaltma miktarı da o oranda artmaktadır. Ek olarak SVM algoritmasını test edebilmek amacıyla özellik seçimi işlemi uygulanmıştır. Bu işlem uygulanırken karar ağacı modeli tarafından oluşturulan özellik önem değerlerine göre özellik seçimi yaklaşımı benimsenmiştir. Özellikleri seçerken 0.0045 eşik değeri karar ağacının doğruluk değerine en yakın değeri verdiği için seçilmiştir. Sonuç olarak 11 özellikten oluşan bir alt veri seti oluşturulmuş ve SVM algoritmasıyla model eğitilirken bu veri seti kullanılmıştır.

8.4.4. Algoritmaların Uygulanması

Bu çalışma kapsamında veri setine sırasıyla uygulanan sınıflandırma algoritmaları şu şekildedir: Karar Ağacı, GBM (gradient boosting machines), lightGBM, XGBoost, Catboost, linear regression ve k-nearest neighbors. Bu algoritmaların hangi parametrelerle eğitildiği maddeler hâlinde aşağıda verilmiştir.

- Karar ağacı algoritması ile model eğitilirken ağacın derinliğinin belirlenmesi modelin ezber yapmaması için önemli bir faktördür.

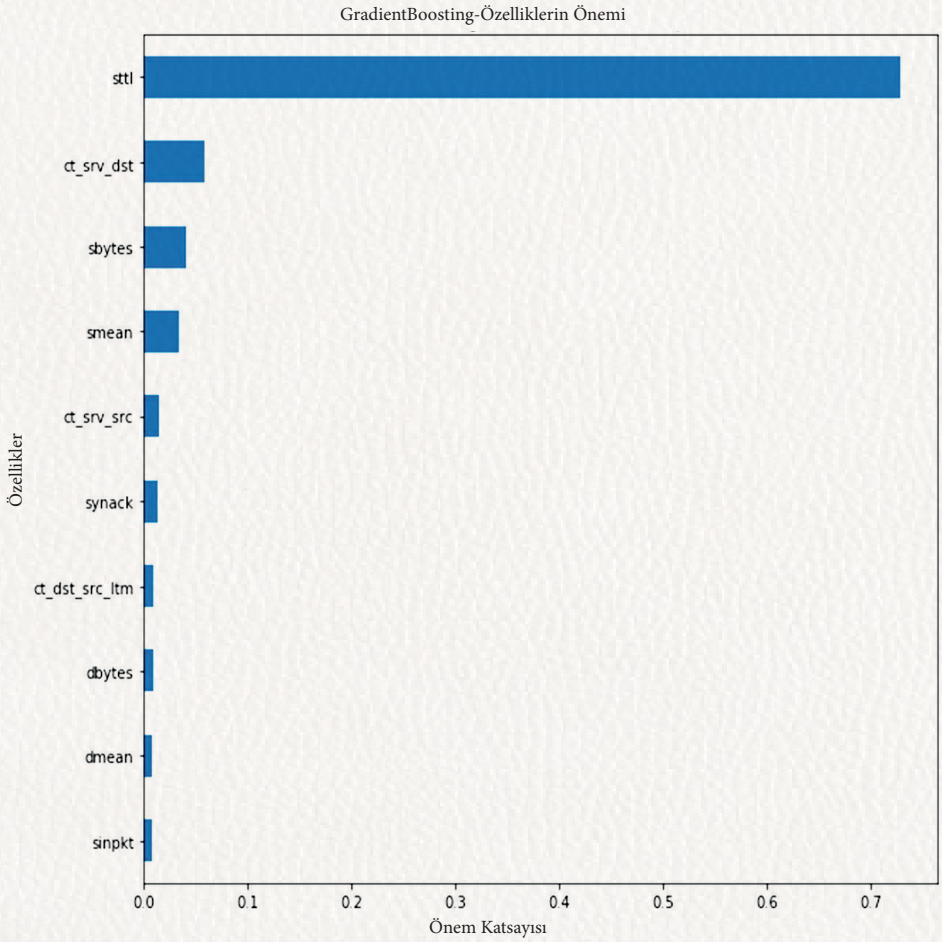
Denemeler sonucunda bu derinlik değeri 10 olarak belirlenmiş ve bu parametre verilerek model eğitilmiştir. Model eğitilirken veri setinin ölçeklendirilmemiş ve boyutu azaltılmamış hâli kullanılmıştır. Algoritmanın uygulanması sonucu özeliklerin önem değerlerinin gösterildiği grafik Şekil 8.11'de verilmiştir. Karar ağaçları özellik önem değerini hesaplarken varsayılan olarak ağaç içindeki ağırlıkları dikkate alınır.



Şekil 8.11. Karar ağacı özellik önem grafiği

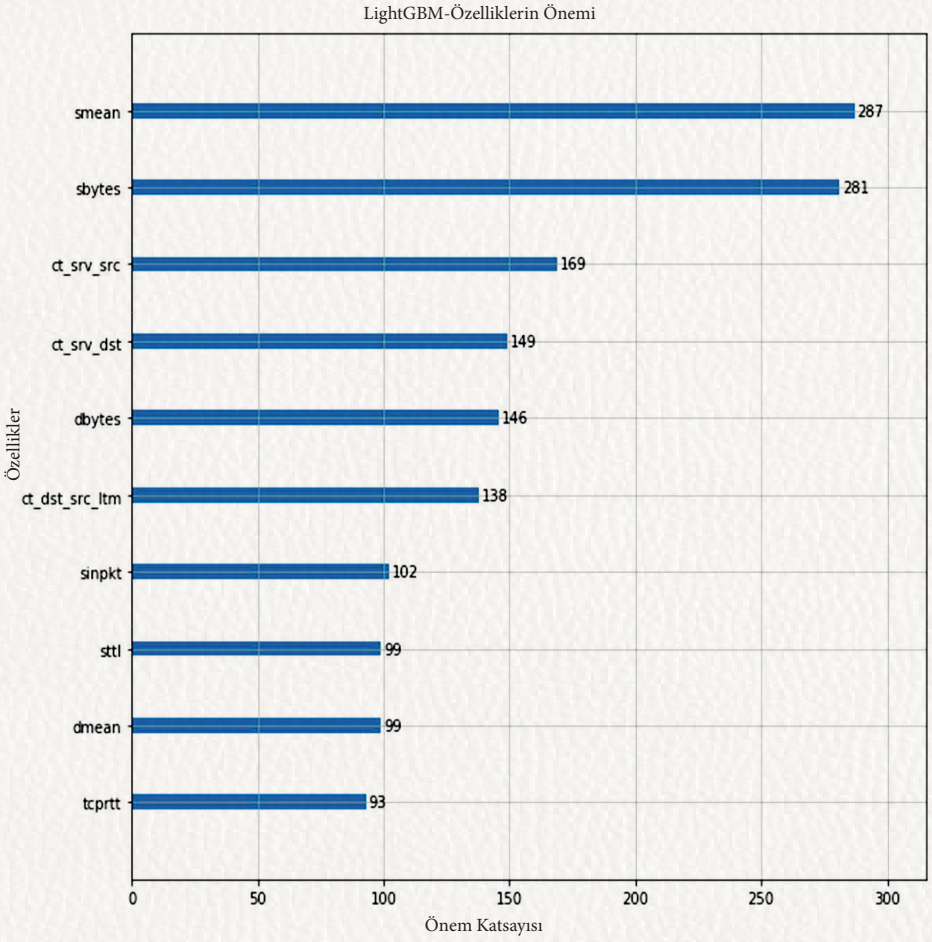
Bu grafiklerde genelde ilk 3 ile 5 özellik bilgilendirici olmaktadır geri kalanın modelin başarısı üzerinde etkisi çok fazla olmamaktadır.

- Gradyan destekli ağaç algoritması ile model eğitilirken karar ağaçlarında olduğu gibi veri setinin ölçeklendirilmemiş ve boyutu azaltılmamış hâli kullanılmıştır. Ek olarak modeller arasında adil ve doğru bir karşılaştırma yapabilmek için ağaç derinliği yine 10 olarak verilmiştir. Algoritmanın uygulanması sonucu özeliklerin önem değerlerinin gösterildiği grafik Şekil 8.12'de verilmiştir.



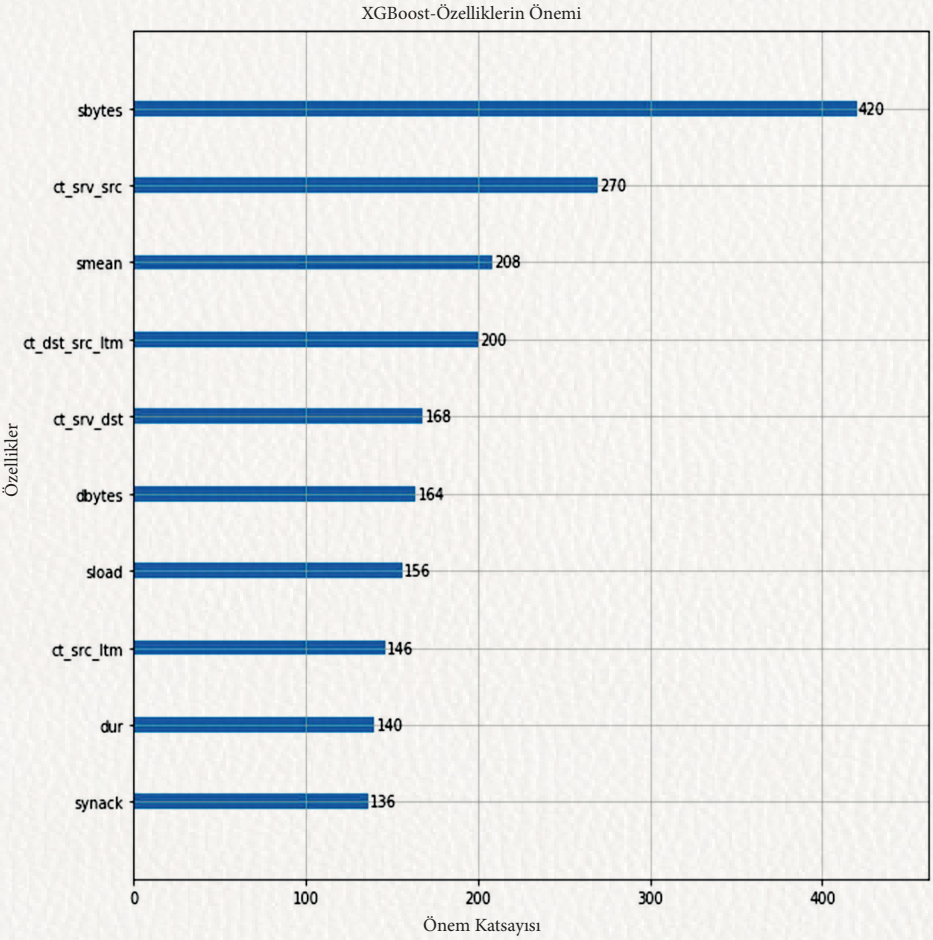
Şekil 8.12. Gradyan destekli makineler özellik önem grafiği

- LightGBM algoritmasıyla yine veri setinin ölçeklendirilmemiş ve boyutu azaltılmamış hâli kullanılmıştır. Modeller arasında adil ve doğru bir karşılaştırma yapabilmek için ağaç derinliği yine 10 olarak verilmiştir. Sınıflandırma yapacağımız veri setinde 0 ve 1 olmak üzere iki sınıf olduğu için sınıflandırma parametresi bu duruma uygun şekilde seçilmiştir. Algoritmanın uygulanması sonucu özeliklerin önem değerlerinin gösterildiği grafik Şekil 8.13'te verilmiştir.



Şekil 8.13. LightGBM özellik önem grafiği

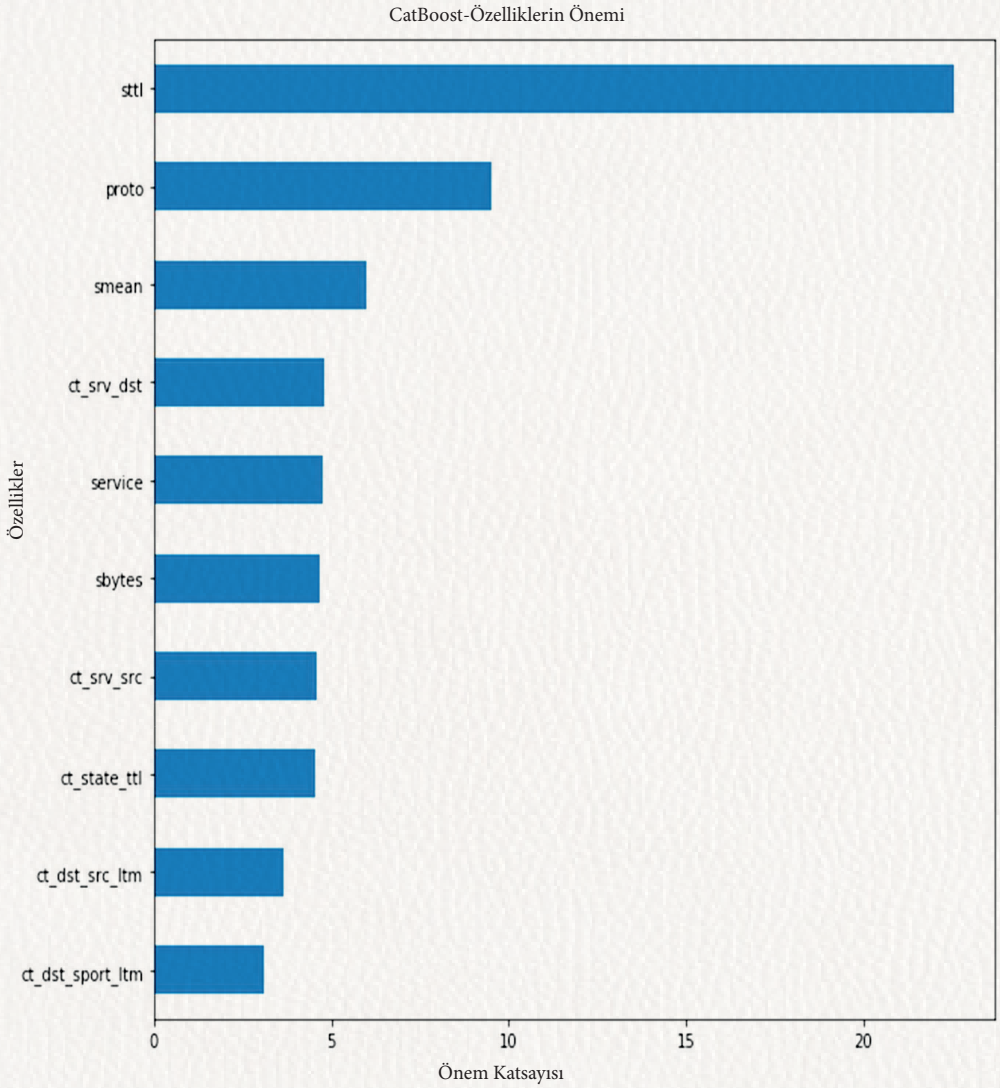
- XGBoost algoritmasıyla model eğitilirken veri setinin ölçeklendirilmemiş ve boyutu azaltılmamış hâli kullanılmıştır. Modeller arasında adil ve doğru bir karşılaştırma yapabilmek için ağaç derinliği yine 10 olarak verilmiştir. Sınıflandırma yapacağımız veri setinde 0 ve 1 olmak üzere iki sınıf olduğu için sınıflandırma parametresi bu duruma uygun şekilde seçilmiştir. Algoritmanın uygulanması sonucu özeliklerin önem değerlerinin gösterildiği grafik Şekil 8.14'te verilmiştir.



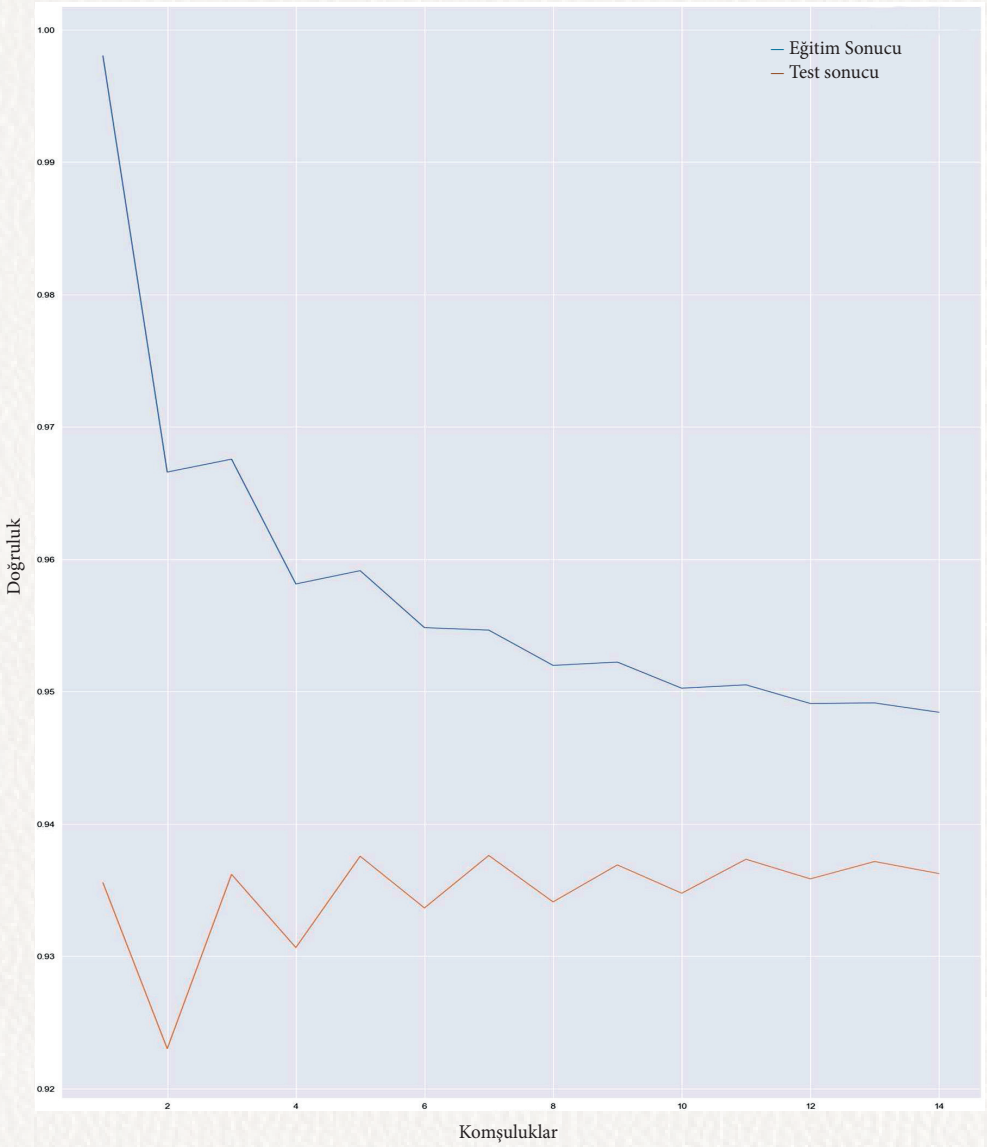
Şekil 8.14. XGBoost özellik önem grafiği

- CatBoost algoritmasıyla model eğitilirken veri setinin ölçeklendirilmemiş ve boyutu azaltılmamış hâli kullanılmıştır. Bu algoritma kategorik veriler üzerinde encoding yapmadan çalışabildiği için one-hot-encoding yapılmamış eğitim setiyle de eğitilmiştir. Modeller arasında adil ve doğru bir karşılaştırma yapabilmek için ağaç derinliği yine 10 olarak verilmiştir. Sınıflandırma yapacağımız veri setinde 0 ve 1 olmak üzere iki sınıf olduğu için sınıflandırma parametresi bu duruma uygun şekilde seçilmiştir. Algoritmanın uygulanması sonucu özeliklerin önem değerlerinin gösterildiği grafik Şekil 8.15'te verilmiştir.
- Naive Bayes algoritması uygulanırken performans karşılaştırmasında eşitliği sağlayabilmek açısından veri seti üzerinde ölçeklendirme ve boyut küçültme işlemleri yapılmadan model eğitilmiştir. Algoritmada Naive Bayes türlerinden Gauss sınıflandırıcı seçilmiştir. Bunun sebebi Bernoulli ve Multinomial sınıflandırıcılara göre daha iyi başarı elde edilmesidir. Bunun dışında herhangi bir parametre kullanılmamıştır.
- SVM algoritmasıyla model eğitilmeden önce karar ağacı tarafından oluşturulan özellik önem değerlerine 0.0045 eşik değeri uygulanarak 11 özellik seçilerek model eğitilmiştir. Eşik değeri seçilirken karar ağacının doğruluk değerine en yakın değeri veren özelliklerin seçimi dikkate alınmıştır. SVM için alt veri kümesinin oluşturulmasının sebebi verinin 194 özellikli hâliyle SVM'in hesaplanmasının çok uzun sürmesi ve sonuca ulaşamamasıdır.
- Doğrusal Regresyon algoritmasıyla veri seti üzerinde ölçeklendirme ve boyut küçültme işlemleri yapıldıktan sonra model eğitilmiştir. Bunun sebebi algoritmanın bu şekilde başarısının daha iyi olmasıdır. Bu algoritmada herhangi bir parametre kullanılmamıştır.
- k-NN algoritmasıyla da veri seti üzerinde ölçeklendirme ve boyut küçültme işlemleri yapıldıktan sonra model eğitilmiştir. Burada mo-

delin başarılı olabilmesindeki önemli nokta k değerinin doğru şekilde seçilmesidir bunun için Şekil 8.16'da yer alan grafik göz önüne alınmıştır.



Şekil 8.15. CatBoost özellik önem grafiği



Şekil 8.16. k-NN eğitim ve test veri setinin başarısının k sayısına göre değişim grafiği

Grafikten görüldüğü üzere k değeri 5 seçildiğinde model için en uygun değer seçilmiş olacaktır.

8.5. TESTLER VE KARŞILAŞTIRMALAR

Bu çalışma kapsamında gerçekleştirilen uygulamada kullanılan danışmanlı makine öğrenmesi algoritmalarının karşılaştırılması için altı metrik kullanılmıştır bunun sebebi ise yalnızca doğruluk oranının modelin başarısını temsil etmede yetersiz kalmasıdır.

8.5.1. Performans Metrikleri

Söz konusu performans metrikleri maddeler hâlinde aşağıda açıklanmıştır. Öncesinde TP, FP, TN, FN değerlerinin ne anlama geldiğini veri setimizden yola çıkarak açıklamak gereklidir.

TP (True Positive – Doğru Pozitif): Anomaliye anomali demektir.

FP (False Positive – Yanlış Pozitif): Anomali olmayana anomali demektir.

TN (True Negative – Doğru Negatif): Anomali olmayana anomali değil demektir.

FN (False Negative – Yanlış Negatif): Anomali olana anomali değil demektir.

- Doğruluk (accuracy), bir niceliğin ölçüm değerinin asıl değerine olan yakınlık derecesidir. Bu çalışmada doğru şekilde sınıflandırılan tüm normal ve saldırı kayıtlarının yüzdesini vermektedir [25]. Accuracy=(TP+TN)/(TP+FP+TN+FN) şeklinde hesaplanmaktadır.
- Kesinlik (precision), aynı şartlardaki ölçümlerin aynı sonucu verme derecesidir. Precision=TP/TP+FP şeklinde hesaplanmaktadır.
- Duyarlılık (recall), kullandığımız veri seti için düşünüldüğünde anomalileri doğru tespit etme oranı olarak söylenir. Recall=TP/TP+FN şeklinde hesaplanır.
- F1 skoru, kesinlik ve duyarlılığın ağırlıklı ortalaması olarak yorumlanabilir, burada F1 skoru 1'de en iyi değerine ve 0'da en kötü puana ulaşır [26]. F1=2*(precision*recall)/(precision+recall) şeklinde hesaplanmaktadır.
- ROC-AUC skoru, Alıcı İşletim Karakteristik Eğrisinin (ROC) altında kalan alanı belirtmektedir. AUC, olası tüm sınıflandırma eşiklerinde toplam performans ölçümü sağlar. Bu değer 0-1 arasında değişmektedir. 0 ise modelin tahminleri %100 yanlıştır. 1 ise modelin tahminleri %100 doğrudur.

- Yanlış pozitif oranı (False positive rate - FPR), aynı zamanda yanlış alarm olarak da adlandırılmaktadır. FPR=FP/FP+TN şeklinde hesaplanmaktadır. FPR'nin yüksek olması istenmeyen bir durumdur.

8.5.2. Algoritmaların Karşılaştırılması

Tüm bu açıklamaların ışığında algoritmaların çalıştırılması sonucu elde edilen değerler Şekil 8.17 ve Şekil 8.18'de görülmektedir. Burada modellerin ezberleme (overfit) veya öğrenememe (underfit) durumu olup olmadığını kontrol edebilmek için hem eğitim hem de test veri setleri için bahsi geçen tüm skorlar hesaplanmıştır.

	accuracy	auc score	precision	recall	f1 score	FPR(False Positive Rate)	execution time
Decision Tree	0.946155	0.923727	0.938339	0.985699	0.961436	0.138245	00:00:02.430524
GradientBoosting Machines	0.982391	0.976775	0.982034	0.992295	0.987138	0.038745	00:04:40.244493
LightGBM	0.960142	0.948871	0.962155	0.980014	0.971002	0.082272	00:00:02.613574
XGboost	0.959087	0.946060	0.958857	0.982056	0.970318	0.089936	00:00:18.397520
CatBoost	0.985592	0.980509	0.984445	0.994556	0.989475	0.033539	00:03:21.591685
One-Hot-Encoded CatBoost	0.991830	0.988663	0.990652	0.997414	0.994022	0.020088	00:03:18.363368
Gaussian Naive Bayes	0.796567	0.760101	0.843589	0.860864	0.852139	0.340662	00:00:00.765525
SVM-RBF Kernel	0.848223	0.776282	0.831239	0.975073	0.897429	0.422510	00:20:25.655032
Linear Regression	0.932046	0.895264	0.911582	0.996901	0.952334	0.206373	00:00:01.411054
K-Nearest Neighbors	0.921032	0.896137	0.922649	0.964928	0.943315	0.172655	00:00:21.962907

Şekil 8.17. Eğitim veri seti performans değerleri

	accuracy	auc score	precision	recall	f1 score	FPR(False Positive Rate)	execution time
Decision Tree	0.944481	0.921745	0.936438	0.985140	0.961436	0.141650	00:00:02.430524
GradientBoosting Machines	0.961619	0.951470	0.964305	0.979767	0.971975	0.076827	00:04:40.244493
LightGBM	0.955887	0.943472	0.957864	0.978088	0.967871	0.091144	00:00:02.613574
XGboost	0.953264	0.938584	0.952994	0.979516	0.966073	0.102348	00:00:18.397520
CatBoost	0.962046	0.951973	0.964634	0.980061	0.972286	0.076116	00:03:21.591685
One-Hot-Encoded CatBoost	0.962217	0.952263	0.964912	0.980019	0.972407	0.075494	00:03:18.363368
Gaussian Naive Bayes	0.794833	0.755290	0.837803	0.865550	0.851450	0.354971	00:00:00.765525
SVM-RBF Kernel	0.843451	0.769621	0.825688	0.975486	0.894358	0.436244	00:20:25.655032
Linear Regression	0.929938	0.892615	0.908966	0.996684	0.950806	0.211453	00:00:01.411054
K-Nearest Neighbors	0.890359	0.860925	0.900329	0.942996	0.921169	0.221145	00:00:21.962907

Şekil 8.18. Test veri seti performans değerleri

Algoritmalar için performans değerleri yorumlandığında CatBoost ve GradientBoosting karar ağacı temelli sistemlerin daha başarılı olduğu görülmektedir. Fakat bu algoritmaların büyük boyutlu veri setlerinde yavaş çalıştıkları saptanmıştır. Bu durum özellikle ağlar için düşünüldüğünde saldırılara karşı hızlı bir şekilde aksiyon almak gerektiği için elverişsiz bir durum ortaya çıkarmaktadır. Bu sebeple bu algoritmalar arasında karşılaştırma yaparken uygulanacak sistemin gereksinimleri göz önünde tutularak karar verilmelidir. Gerçek hayat senaryoları düşünüldüğünde anomali tabanlı çalışan bir ağ saldırı tespit sistemine makine öğrenmesi algoritmasıyla çalışan bir yapı entegre ederek sistemin başarısını arttırabiliriz. Bu durumda şu üç kriter önemli olarak karşımıza çıkmaktadır. Birincisi ağlar gibi çok büyük miktarda veri üreten bir sistemin verilerini hızlı bir şekilde işleyip modeli eğitebilmek. İkincisi eğittiğimiz modelde mümkün olduğunca yüksek doğruluk değerini yakalayabilmek. Üçüncüsü ise yanlış alarmlarla mümkün olduğunca az karşılaşmak. Bazı durumlarda bu üç kriterin biri diğerine göre daha önemli olabilmektedir. Örnek vermek gerekirse bir IDS üzerinden akan trafiğin bir saldırı içerip içermediğini hızlı bir şekilde anlayıp bir an önce saldırıya karşı tedbir alınabilmesi açısından yanlış alarm üretmesi durumuna göre daha önemlidir. Çünkü kritik sistemlerin güvenliğini sağlamak için bu noktada yanlış alarmlara tolerans gösterilebilmelidir.

8.6. SONUÇ VE DEĞERLENDİRMELER

Bu kitap bölümünde, temel olarak anomali tespitinin yapay zekâ yaklaşımlarıyla nasıl belirlenebileceği, bir sistemdeki veya verideki beklenmedik durum veya desenlerin bulunması için yapay zekâ tekniklerinin nasıl kullanıldığı verilmiştir. Burada sunulan anomali tespiti çözüm yaklaşımının, ağ saldırı tespiti, sahtekârlık veya dolandırıcılık tespiti, endüstriyel casusluk veya hasar tespiti gibi birçok alanda uygulanabileceği, anomali tespitinde farklı makine öğrenmesi algoritmaları ve yapılarının kullanılabileceği gösterilmiş, farklı veri setleri üzerinde çalışmalar yapılarak bunların karşılaştırılması yapılmıştır.

Bu bölümde farklı veri setleri üzerinde çeşitli makine öğrenmesi algoritmaları kullanılarak anomali tabanlı ağ saldırı tespitinde hangi yöntemlerin daha etkili sonuçlar verdiği noktasında bir çalışma yapılarak, mevcut mo-

deller karşılaştırılmıştır. Danışmanlı öğrenme sınıflandırma algoritmalarından Naive Bayes, Destek SVM, lineer regresyon, k-NN en yakın komşu, karar ağaçları, gradyan destekli makineler, XGBoost, LightGBM ve CatBoost olmak üzere dokuz farklı algoritma ile UNSW-NB15 adlı ağ trafik verileri kullanılarak test edilmiş ve elde edilen sonuçlar, modellerin eğitilmesi ve test edilmesi sonucu hesaplanan performans metrikleri detaylı olarak verilmiştir. Sonuç olarak;

- CatBoost, GBM, LightGBM algoritmalarının diğerlerine göre daha başarılı sonuçlar verdiği görülmüştür.
- Kullanılacak algoritmaların performanslarının değerlendirilmesinde, uygulanacak sistemin gereksinimleri en önemli faktör olup, tasarımda göz önünde bulundurulmalıdır.
- Algoritmaların eğitimi için farklı sürelere ihtiyaç vardır.
- Bu çalışma kapsamında test edilen ağlarda anomali tespitinde makine algoritmalarıyla modellerin eğitimi gerçekleştirilmiştir. Elde edilen sonuçlar ikili sınıflandırmada makine öğrenmesi algoritmalarının başarısını göstermiştir. Fakat ağ saldırı tespit sistemlerinin daha iyi performansla çalışabilmesi için yalnızca anomali tespiti yeterli olmamakla birlikte saldırı türlerinin de doğru bir şekilde tespit ediliyor olması gerekmektedir.
- Burada sunulan çözümlerin, özellikle hem saldırıların tespiti hem de anomalilerin belirlenmesinde önemli katkılar sağlayacağı açıktır. Bu tür zeki çözümlerin bilgi güvenliği ihlal eden anomalilerin tespitinin yanında genel olarak yapılan saldırıların ayrıştırılmasına kadar pek çok alanda başarı ile kullanılabileceği değerlendirilmektedir. Ayrıca, siber güvenlikte, saldırıların tespitinde yapay zekâ yaklaşımlarının kullanılmasını arttıracağı, konuya olan ilgiyi yükselteceği ve farklı bakış açıları kazanılmasını sağlayacağı açıktır.
- Son zamanlarda, saldırı türlerinin de başarılı bir şekilde tespit edilebilmesi için derin öğrenme yaklaşımlarının kullanılmasının bu başarıları arttıracağı değerlendirilmektedir.

KAYNAKLAR

[1] Ahmed, Mohiuddin, Mahmood, Abdun ve Hu, Jiankun. (2015). A Survey of Network Anomaly Detection Techniques. Journal of Network and Computer Applications. 60. 19-31. 10.1016/j.jnca.2015.11.016.

[2] A. Chandola, V. Chandola, V. Kumar. "Anomaly Detection: A Survey", ACM Comput. Surv., 41 (3), 2009, doi:10.1145/1541880. 1541882

[3] Bhuyan, M. H., Bhattacharyya, D. K. ve Kalita, J. K. (2014). Network Anomaly Detection: Methods, Systems and Tools. *IEEE Communications Surveys & Tutorials*, *1*(16), 303-336.

[4] Lin J, Keogh E, Fu A, Van Herle H. Approximations to magic: finding unusual medical timeseries. In: Proceedings of the 18th IEEE symposium on computer-based medical systems, CBMS'05, IEEE Computer Society, Washington, DC, USA; 2005.p.329–334.

[5] Sarıkaya, A. (2018). Anomaly-based cyber intrusion detection system with ensemble classifier (Master's thesis).

[6] Saranya, T., Sridevi, S., Deisy, C., Chung, T. D. ve Khan, M. A. (2020). Performance Analysis of Machine Learning Algorithms in Intrusion Detection System: A Review. Procedia Computer Science, 171, 1251-1260.

[7] Kumar, D. P., Amgoth, T. ve Annavarapu, C. S. R. (2019). Machine learning algorithms for wireless sensor networks: A survey. Information Fusion, 49, 1-25.

[8] Eskin E, Arnold A, Prerau M, Portnoy L, Stolfo S. A geometric framework for unsupervised anomaly detection. In: Barbará D, Jajodia S (editörler). Applications of data mining in computer security, Adv Inf Secur, vol. 6. Springer US, 2002. p. 77–101.

[9] Nour Moustafa ve Jill Slay (2016) The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set, Information Security Journal: A Global Perspective, 25: 1-3, 18-31, DOI: 10.1080/19393555.2015.1125974

[10] Kumar, V., Sinha, D., Das, A. K., Pandey, S. C. ve Goswami, R. T. (2020). An integrated rule based intrusion detection system: analysis on UNSW-NB15 data set and the real time online dataset. Cluster Computing, 23 (2), 1397-1418.

[11] Canbek, G. ve Sagiroglu, S (2007). Bilgisayar Sistemlerine Yapılan Saldırılar ve Türleri: Bir İnceleme {Attacks against Computer Systems and Their Types: A Review Study}. Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi. 23. 1-12.

[12] Lv, L., Wang, W., Zhang, Z. ve Liu, X. (2020). A novel intrusion detection system based on an optimal hybrid kernel extreme learning machine. Knowledge-Based Systems, 105648.

[13] Liao, H. J., Lin, C. H. R., Lin, Y. C. ve Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications, 36 (1), 16-24.

[14] Abdullah A. Mohamed, "Design Intrusion Detection System Based on Image Block Matching", International Journal of Computer and Communication Engineering, IACSIT Press, Vol. 2, No. 5, September 2013.

[15] Taha, A. ve Hadi, A. S. (2019). Anomaly detection methods for categorical data: A review. ACM Computing Surveys (CSUR), 52 (2), 1-35.

[16] Müller A. C. ve S. Guido, (2016). Introduction to machine learning with Python: a guide for data scientists, first edition, " O'Reilly Media, Inc."

[17] Han, J., Kamber, M. ve Pei, J. (2006). Data mining concepts and techniques, second edition Morgan Kaufmann Publishers

[18] Chen, Tianqi ve Guestrin, Carlos. (2016). XGBoost: A Scalable Tree Boosting System. 785-794. 10.1145/2939672.2939785.

[19] XGBoost Documentation. URL: https://xgboost.readthedocs.io/en/latest/, Son Erişim Tarihi: 22 Aralık 2019

[20] Welcome to LightGBM's documentation! URL: https://lightgbm.readthedocs.io/en/latest/, Son Erişim Tarihi: 22 Aralık 2019

[21] Ke, G., Meng, Q., Finley, T., Wang, T., Chen, W., Ma, W., Ye, Q. ve Liu, T. (2017). LightGBM: A Highly Efficient Gradient Boosting Decision Tree. Neural Information Processing Systems (NIPS).

[22] Prokhorenkova, L., Gusev, G., Vorobev, A., Dorogush, A. V. ve Gulin, A. (2018). CatBoost: unbiased boosting with categorical Features.

[23] Moustafa, Nour ve Slay, Jill. (2015). UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). 10.1109/MilCIS.2015.7348942.

[24] The UNSW-NB15 Dataset Description. URL: https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/ADFA-NB15-Datasets/, Son Erişim Tarihi: 24 Aralık 2019

[25] Moustafa, N., Slay, J. ve Creech, G. (2017). Novel Geometric Area Analysis Technique for Anomaly Detection Using Trapezoidal Area Estimation on Large-Scale Networks. IEEE Transactions on Big Data, 5, 481-494.

[26] Sklearn.metrics-Scikit-learn. URL:https://scikitlearn.org/stable/modules/generated/sklearn.metrics.f1_score.html#sklearn.metrics.f1_score, Son Erişim Tarihi:24 Aralık 2019

[27] Sağıroğlu, S. E. N. Yolaçan, U. Yavanoğlu, Zeki Saldırı Tespit Sistemi Tasarımı ve Gerçekleştirilmesi, Gazi Üniv. Müh. Mim. Fak. Dergisi, Cilt 26, No 2, 325-340, 2011

Bölüm 9

KRİPTOGRAFİK BLOK ŞİFRELERİN MAKSİMUM UZAKLIKLA AYRILABİLEN YAYILIM TABAKALARININ TASARIMI

Meltem Kurt Pehlivanoğlu - Elif Bilge Kavun

Bu bölümde, kriptografideki blok şifreleme algoritmalarının en önemli bileşenlerinden biri olan yayılım tabakalarının ayrıntılı incelemesine yer verilmiştir. Kriptografik açıdan güvenli yayılım tabakalarının tasarımında kullanılan yöntemler ve bu yöntemlerin dayandırıldığı yapılar kapsamlı olarak sunulmuştur. Blok şifreleme algoritmalarında çoğunlukla yayılım tabakası olarak kullanılan ve maksimum yayılma sağlayan MDS (Maximum Distance Separable - Maksimum Uzaklıkla Ayrılabilen) matrislerin üretimi için geliştirilen farklı tasarım yöntemleri ve bu yöntemlere ait matematiksel altyapı verilmiştir. Bunun yanı sıra literatürde yer alan yerel (local) ve genel (global) optimizasyon teknikleri karşılaştırmalı olarak sunulmuştur.

9.1. GİRİŞ

Kerckhoffs'un Prensibi'ne göre [1] bir kriptosistemin güvenliği, kullanılan algoritmanın veya parametrelerin gizliliğine dayanmaz. Bu ilke güvenliğin sadece kriptosistemde kullanılan anahtarın gizliliğine bağlı olacağı anlamına gelir. Blok şifreler, seçilen gizli anahtar yardımıyla, sabit uzunluktaki bloklar (bit dizileri) kümesine şifreleme/şifre çözme işlemi uygulayan algoritmalardır. Blok şifrelerin tasarım prensibi Shannon'un önerdiği karıştırma (confusion) ve yayılma (diffusion) tekniklerine dayanır. Bu teknikler bir şifreyi istatis-

tiksel saldırılardan korumaya yarar. Karıştırma, gizli anahtar ile şifreli metin arasındaki ilişkiyi gizlemeyi amaçlar. Diğer bir ifadeyle; gizli anahtar öyle bir şekilde kullanılır ki, bir saldırgan açık metnin istatistiksel dağılımını bilse veya çok sayıda düz metin/şifreli metin çiftlerine sahip olsa bile, gizli anahtarı hâlâ çıkaramaz. Yayılma ise açık metinle şifreli metin arasındaki ilişkiyi gizler. Şifreli metnin her bir parçası mümkün olduğunca açık metne bağlı olmalıdır ki; açık metinde yapılacak çok küçük bir değişiklik (örneğin 1 bit değişim) şifreli metin üzerinde olabildiğince fazla değişim sağlamalı, diğer bir ifadeyle bu değişim maksimum yayılmalıdır [2]. Blok şifreler, temelde doğrusal olmayan tabaka (confusion layer), yayılım tabakası (diffusion/permutation layer) ve anahtar planlama algoritmasının (key scheduling algorithm) yer aldığı döngü (round) adı verilen yapılardan oluşurlar. Her döngüde farklı döngü anahtarı (alt anahtarlar) kullanılır ve bu anahtarlar anahtar planlama algoritması kullanılarak üretilir. Karıştırmanın sağlandığı doğrusal olmayan tabakada şifrenin tek doğrusal olmayan yapısı olarak yer değiştirme kutuları (Substitution-boxes – S-kutuları) kullanılırken, yayılmayı sağlayan yayılım tabakasında ise doğrusal dönüşümler kullanılır. Açık metin üzerinde yapılan bit değişimlerinden olabildiğince fazla sayıdaki S-kutusunun etkilenmesi beklenir. Bu bit değişiminden etkilenen S-kutusu sayısı, aktif S-kutusu olarak bilinir ve minimum aktif S-kutusu sayısının maksimum olması beklenir. S-kutuları ile ilgili literatürdeki çalışmalar incelendiğinde bu alanın iyi çalışıldığı görülebilir ancak kriptografik açıdan güçlü ve verimli yayılım tabakalarının tasarımı hâlâ açık bir problemdir [3].

Blok şifreler farklı tasarım mimarileri kullanılarak tasarlanabilir, en temel iki tasarım mimarisi Feistel Ağları (Feistel Networks) ile Yer değiştirme ve Permütasyon Ağlarıdır (Substitution Permutation Networks–SPN). Feistel mimarisinde döngü bloğu ikiye bölünerek dallara ayrılır ve bu mimaride dalın yarısı işlenirken, SPN mimarisinde döngü bloğunun tamamı işlenir. Her iki mimariye ilişkin karşılaştırmalı kapsamlı bilgiye [2]'den erişilebilir.

Kriptografik açıdan güvenli ve verimli yayılım tabakalarının tasarımı önemlidir. İyi yayılımın sağlanması için bilinen iki genel tasarım yaklaşımı vardır; ad – hoc (geçici) [4] ve wide–trail (geniş–iz) [5]. Geçici yaklaşımda optimum izlerin bulunması için bilgisayar destekli araçlar gerekir. Geniş–iz yaklaşımında ise doğrusal ve diferansiyel saldırılara [6] karşı dayanıklı tasarım sağlanması için; kaynakların büyük boyutlu S-kutuları için kullanımı yerine, yüksek yayılımın sağlanacağı doğrusal dönüşümlere (diğer bir ifadeyle yayılım taba-

kalarına) harcanması amaçlanır. Kaynakların kriptografik açıdan güvenli ve verimli yayılım tabakalarının tasarımı için kullanımı, aktif S-kutusu sayısını da arttıracaktır. Aktif S-kutularının hesaplanması ile ilgili kapsamlı bilgiye [7]'den erişilebilir. Geniş–iz tasarım yaklaşımı yayılım tabakalarının tasarımının önemini vurgulasa da uygun sayıda aktif S-kutusu ile verimli ve güvenli yayılım tabakalarının nasıl tasarlanması gerektiği önemli bir araştırma problemidir. Bunun yanında kaynak kısıtlı cihazlar (kısıtlı hesaplama gücü, bellek kapasitesi, güç kaynağı) için önerilen hafif sıklet (lightweight) kriptosistemlerin yayılım tabakalarının tasarımı da literatürde yer alan bir diğer açık problemdir [8].

Bir blok şifrede yayılım tabakaları farklı yapılar kullanılarak oluşturulabilir; bit permütasyonlarının kullanımı, dalların karıştırılması (the shuffle of the branches), doğrusal cebir tabanlı (linear algebra based) yapıların kullanılması [2] bu yapılara örnek olarak gösterilebilir. Bit permütasyonlarında S-kutusu çıktı bitleri, bit permütasyonları kullanılarak karıştırılır. Bit permütasyonları, düşük maliyetli (low–cost) donanım hedefli blok şifreler için uygundur. Bu yapılarda bir çıkış biti bir sonraki katmanın yalnızca (en fazla) tek bir giriş bitini etkiler, bu nedenle yayılım oldukça yavaştır ve fazla sayıda döngüye ihtiyaç duyulur. PRESENT [9], PRINTcipher [10], Khazad [11], Anubis [12], ICEBERG [13] blok şifreleri yayılım tabakalarında bit permütasyonu kullanırlar. Dalların karıştırılması Feistel mimarisindeki blok şifreler için kullanılan yöntemlerden biridir ve dalların dairesel olarak kaydırılması işlemidir. DES [14], SAFER family [15], [16] ve FROG [17] blok şifreleri yayılım tabakalarında bu yöntemi kullanırlar. Doğrusal cebir tabanlı yayılım tabakaları, elemanları sonlu cisim üzerinde tanımlı matrisler olarak ifade edilebilir [2]. Shark [18], SQUARE [19], AES [20], Twofish [21], Camellia [22] blok şifreleri yayılım tabakası olarak doğrusal cebir tabanlı yayılım matrislerini kullanırlar.

Blok şifrelerde kullanılan yayılım tabakalarının tasarımındaki hedef en iyi yayılmayı (perfect diffusion) sağlamaktır. Cebirsel yayılım tabakaları ele alındığında, bir blok şifredeki en iyi yayılma; çoklu permütasyonu sağladığı için MDS matrislerin kullanımıyla elde edilir [23]. Bu nedenle maksimum yayılmayı sağlayan MDS matrislerin tasarımı literatürde çalışılan önemli açık problemlerden biridir [24].

Bu bölümde blok şifrelerde kullanılan en önemli yayılım tabakası tasarımlarından biri olan MDS matrislere ait matematiksel altyapı ve bu matrislerin

tasarım yöntemleri verilmiştir. Ayrıca bu yöntemler yerel ve genel optimizasyon teknikleri açısından karşılaştırmalı olarak sunulmuştur.

Çalışmanın ilerleyen bölümleri şu şekilde düzenlenmiştir; Bölüm 9.2'de MDS matrisler için matematiksel altyapı verilmiştir. Bölüm 9.3'te ise MDS matrisler için geliştirilen farklı tasarım yöntemleri sunulmuştur. Bölüm 9.4'te, Bölüm 9.3'te verilen tasarım yöntemleri yerel ve genel optimizasyon açısından değerlendirilmiştir. Son bölümde ise çalışmada verilen kapsamlı bilgiler değerlendirilerek özetlenmiştir.

9.2. MDS MATRİSLER İÇİN MATEMATİKSEL ALTYAPI

Bu bölümde MDS matrislerin dayandığı matematiksel tanımlar ve önermelere yer verilmiştir. MDS matrislerle ilgili detaylı tanımlamalara ve önermelere [25]'ten erişilebilir.

Tanım 9.1. (Sonlu Cisim): Sonlu sayıda elemanı olan cisim sonlu cisim olarak ifade edilir. $\mathbb{F}$ sonlu cisim ve m pozitif sayı olmak üzere $\mathbb{F}_{2^m}$ sonlu cismi, elemanları $\{0,1\}$ 'den oluşan $\mathbb{F}_2$ sonlu cisminin m. dereceden genişletilmiş bir cismidir ve 2^m elemana sahiptir.

$\mathbb{F}_{2^m}$ sonlu cisminin her bir elemanı katsayıları $\mathbb{F}_2$ cisminde tanımlı ve derecesi $m-1$ olan bir polinom şeklinde ifade edilebilir. α ilkel eleman ve $x \in \mathbb{F}_{2^m}$ olmak üzere; x elemanının polinom tabanlı gösterimi Eşitlik (9.1)'deki gibidir.

$$x_{m-1}\alpha^{m-1} + x_{m-2}\alpha^{m-2} + \ldots + x_1\alpha + x_0 \tag{9.1}$$

Önerme 9.2. (Singleton Sınırı): Bir doğrusal kod C $[n,k,d]$ için Singleton sınırı $d \leq n-k+1$'dir.

Tanım 9.3. (MDS Kod): C $[n,k,d]$ kodu için $d = n-k+1$ ise C MDS koddur denir.

Önerme 9.4. (MDS Matris): C $[n,k,d]$ kodu, I $k \times k$ boyutlu birim matris, A $k \times (n-k)$ boyutlu matris ve $G = [I \mid A]$ üreteç matris olmak üzere, C ancak ve ancak A matrisinin satır ve sütunlarını oluşturan tüm alt kare matrislerin determinantı sıfırdan farklı (tekil olmayan matris) ise MDS koddur ve bu durumda A matrisi MDS matristir denir.

Bir blok şifrede iyi yayılma istenirken bir taraftan da şifrenin hızlı olması beklenir. Bu nedenle bu iki metrik arasında denge sağlamak amaçlı, optimum yayılmayı (optimal diffusion) hedefleyen yayılım matrislerinin kullanılması

gerekir. Daemen [5] optimum yayılmayı dal sayısı (branch number) metriğiyle ifade etmiştir ve dal sayısı β gösterimi ile tanımlanabilir. θ tersi alınabilir (invertible) doğrusal dönüşüm olmak üzere, θ'nın dal sayısı β_θ Eşitlik (9.2)'deki gibidir.

$$\beta_\theta = \min_{\alpha \neq 0} \{ wt(\alpha) + wt(\theta(\alpha)) \} \tag{9.2}$$

$wt(\alpha)$; α'nın Hamming ağırlığını (1'e eşit olan elemanların sayısı) ifade eder. $wt(\alpha) \leq n$, her θ için, eğer $wt(\alpha) = 1$ ise bu da $\beta_\theta \leq n+1$ olduğu anlamına gelir. θ tersi alınabilir bir doğrusal dönüşümü için optimum dal sayısı $\beta_\theta = n+1$'dir [5].

Dal sayısı, bir matrisin ifade ettiği doğrusal dönüşümün yayılma gücünü tanımlar. Matrisin kendisinin dal sayısı (β_d) diferansiyel yayılmayı ölçerken, matrisin devriğinin (transpose) dal sayısı (β_l) doğrusal yayılmayı ölçer. Dal sayısı, en kötü durumdaki (worst-case) yayılmayı ölçer, şöyle ki iki ardışık döngüdeki aktif S-kutusu sayısı için alt sınır değerini (en kötü durumdaki minimum aktif S-kutusu sayısı) verir [2]. Tanım 9.5'te diferansiyel dal sayısı, Tanım 9.6'da ise doğrusal dal sayısı eşitlikleri verilmiştir.

Tanım 9.5. (Diferansiyel Dal Sayısı): $n \times n$ boyutlu A matrisinin diferansiyel dal sayısı;

$$\beta_d = \min \left\{ wt(x) + wt(A \cdot x^T) \mid x \in (\{0,1\}^m)^n, x \neq 0 \right\} \tag{9.3}$$

olarak ifade edilmektedir.

Tanım 9.6. (Doğrusal Dal Sayısı): $n \times n$ boyutlu A matrisinin doğrusal dal sayısı;

$$\beta_l = \min \left\{ wt(x) + wt(A^T \cdot x^T) \mid x \in (\{0,1\}^m)^n, x \neq 0 \right\} \tag{9.4}$$

olarak ifade edilmektedir.

Bir doğrusal dönüşüm için optimum dal sayısı $\beta_\theta = n+1$ olduğundan, $\beta_d(A)$ ve $\beta_l(A)$ dal sayılarının maksimum değeri $n+1$'dir. Bu değer MDS kodlarla oluşturulan doğrusal dönüşümlerle sağlanabilir, bu da MDS matrislerin optimum yayılma sağladığını kanıtlar [5].

MDS matrisler için önemli özellikler aşağıdaki gibi verilebilir;

- $n \times n$ boyutlu M matrisi ancak ve ancak satır ve sütunlarını oluşturan tüm alt kare matrisleri tekil olmayan matris ise ve M matrisinin elemanları 0'dan farklı ise MDS matristir.

- $n \times n$ boyutlu M matrisi MDS matris ise, M matrisinin tüm alt kare matrislerinin rank'ı tam (full) rank'tır.
- $n \times n$ boyutlu M matrisi MDS matris ise, M matrisinin tüm alt kare matrisleri de MDS matristir.
- $n \times n$ boyutlu M matrisi MDS matris ise, M matrisinin devriği (transpose) M^T MDS matristir.
- $n \times n$ boyutlu M matrisi MDS matris ise, M matrisinin tersi M^{-1} matrisi MDS matristir.
- $n \times n$ boyutlu M MDS matrisinin herhangi bir satır veya sütunu herhangi bir c $(c \in \mathbb{F}_{2^m}, c \neq 0)$ sabitiyle çarpıldığında MDS özelliği korunur.
- $n \times n$ boyutlu M MDS matrisinin diferansiyel $\beta_d(M)$ ve doğrusal $\beta_l(M)$ dal sayıları $n+1$'dir.

Bunun yanında tersi kendisine eşit (involutory) ve ortogonal (orthogonal) yapılar, MDS matrislerin tasarımı için önemlidir. Tersi kendisine eşit ve ortogonal MDS matrisler kullanılarak blok şifrelerin verimli donanım ve yazılım uygulamaları gerçeklenebilir. Bu nedenle tersi kendisine eşit veya ortogonal verimli MDS matrislerin bulunması önemli bir çalışma alanıdır [26]. Tersi kendisine eşit ve ortogonal matris tanımları sırasıyla Tanım 9.7 ve Tanım 9.8'de verilmiştir.

Tanım 9.7. (Tersi Kendisine Eşit Matris): I $n \times n$ boyutlu birim matris olmak üzere, $n \times n$ boyutlu A matrisi eğer $A^2 = I$ yani $A^{-1} = A$ koşulunu sağlıyorsa bu matrisin tersi kendisine eşittir.

Tanım 9.8. (Ortogonal Matris): I $n \times n$ boyutlu birim matris olmak üzere, $n \times n$ boyutlu A matrisi eğer $AA^T = I$ yani $A^{-1} = A^T$ koşulunu sağlıyorsa bu matris ortogonal matristir.

Verimli yayılım matris tasarımıyla, bir yayılım matrisinin özellikle donanım uygulaması maliyetinin azaltılması amaçlanır. Donanım maliyeti iki önemli metrikle ölçülebilir; XOR (Exclusive Or) [27] sayısı ve derinlik [24]. Yayılım matrisinin donanım uygulamasında kullanılacağı devredeki XOR sayısının azaltılması; devrenin alanını (chip area) ve güç tüketimini (power consumption) azaltırken, devre derinliğinin azaltılması ise gecikmeyi azaltarak (low latency) daha hızlı devrelerin tasarımını sağlar [28]. Azaltılmış devre alanı, azaltılmış güç tüketimi ve hızlı devre tasarımına sahip yayılım matrisleri; ha-

fif sıklet kriptosistemlerin yayılım tabakaları için gereklidir. XOR sayısı ve derinlik metrikleri tanımları sırasıyla, Tanım 9.9 ve Tanım 9.10'da verilmiştir.

Tanım 9.9. (XOR Sayısı): $p(x)$ $\mathbb{F}_{2^m}$ sonlu cismi üzerinde indirgenemez polinom, $a \in \mathbb{F}_{2^m} / p(x)$ ve $b \in \mathbb{F}_{2^m} / p(x)$ olmak üzere, $XOR(a)$, a elemanını keyfi bir b elemanıyla çarpmak için gereken XOR sayısı olarak ifade edilir.

Örnek 9.10: $\mathbb{F}_{2^4}$ sonlu cismi üzerinde, α ilkel eleman ve $p(x)$ $x^4 + x + 1$ (0×13) indirgenemez polinomu olmak üzere, $\mathbb{F}_{2^4} / (0 \times 13)$ sonlu cismi üzerinde herhangi bir $x \in \mathbb{F}_{2^4}$ elemanı için Eşitlik (9.1)'den faydalanılarak $x = (x_3, x_2, x_1, x_0)$ olmak üzere, $x_3\alpha^3 + x_2\alpha^2 + x_1\alpha + x_0$ şeklinde yazılabilir ve bu sonlu cisim üzerinde 9_h $(= \alpha^3 + 1)$ elemanının herhangi bir x elemanı ile çarpımı;

$$x_3\alpha^3 + x_2\alpha^2 + x_1\alpha + x_0 \rightarrow (\alpha^3 + 1)(x_3\alpha^3 + x_2\alpha^2 + x_1\alpha + x_0) \bmod (0 \times 13)$$

$= x_3\alpha^6 + x_3\alpha^3 + x_2\alpha^5 + x_2\alpha^2 + x_1\alpha^4 + x_1\alpha + x_0\alpha^3 + x_0$, burada (0×13) indirgenemez polinomu altında $\alpha^6 = \alpha^3 + \alpha^2, \alpha^5 = \alpha^2 + \alpha, \alpha^4 = \alpha + 1$ olduğundan;

$$= x_3\alpha^3 + x_3\alpha^2 + x_3\alpha^3 + x_2\alpha^2 + x_2\alpha + x_2\alpha^2 + x_1\alpha + x_1 + x_1\alpha + x_0\alpha^3 + x_0$$

$$= \cancel{x_3\alpha^3} + x_3\alpha^2 + \cancel{x_3\alpha^3} + \cancel{x_2\alpha^2} + x_2\alpha + \cancel{x_2\alpha^2} + \cancel{x_1\alpha} + x_1 + \cancel{x_1\alpha} + x_0\alpha^3 + x_0$$

$$= x_0\alpha^3 + x_3\alpha^2 + x_2\alpha + x_1 + x_0$$

$$= (x_0)\alpha^3 + (x_3)\alpha^2 + (x_2)\alpha + (x_1 \oplus x_0)$$

olarak elde edilir. Buradan $(\alpha^3 + 1)$ elemanının herhangi bir x elemanı ile çarpımı için gereken XOR sayısı $XOR(\alpha^3 + 1) = 1$'dir.

$p(x)$ $\mathbb{F}_{2^m}$ sonlu cismi üzerinde bir indirgenemez polinom, $a \in \mathbb{F}_{2^m} / p(x)$ sonlu cismi üzerinde tanımlı herhangi bir eleman olmak üzere, a elemanı $\mathbb{F}_2$ sonlu cismi üzerinde karşılığı olan ikili matrisle ifade edilebilir. Bu gösterim sayesinde blok şifrelerin yayılım tabakalarında kullanılacak yayılım matrisi elemanlarının $\mathbb{F}_2$ sonlu cismi üzerinde ikili matris karşılıkları kullanılarak, matrisin donanım devresinin giriş $(x_0, x_1, \ldots x_k)$ ve çıkış $(y_0, y_1, \ldots y_k)$ haritalaması elde edilir.

$\mathbb{F}_{2^4} / (0 \times 13)$ sonlu cismi üzerinde tanımlı $(\alpha^3 + 1)$ elemanı, 4×4 ikili matris karşılığıyla $\mathbb{F}_2$ cismi üzerinde Eşitlik (9.5)'teki gibi ifade edilebilir;

$$= \underbrace{(x_0)}_{y_3}\alpha^3 + \underbrace{(x_3)}_{y_2}\alpha^2 + \underbrace{(x_2)}_{y_1}\alpha + \underbrace{(x_1 \oplus x_0)}_{y_0} \rightarrow \begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} . \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix} \rightarrow \begin{matrix} y_0 = x_0 \oplus x_1 \\ y_1 = x_2 \\ y_2 = x_3 \\ y_3 = x_0 \end{matrix} \quad (9.5)$$

Örnek 9.11: $\mathbb{F}_{2^4}$ sonlu cismi üzerinde, α ilkel eleman ve $p(x)$ $x^4 + x + 1$ (0×13) indirgenemez polinomu olmak üzere, $\mathbb{F}_{2^4}/(0\times13)$ sonlu cismi üzerinde 4×4 boyutlu

$$A = \begin{bmatrix} 3_h & 2_h & 1_h & 3_h \\ 8_h & 9_h & 2_h & 2_h \\ 9_h & 8_h & 3_h & 2_h \\ 2_h & 2_h & 3_h & 1_h \end{bmatrix} = \begin{bmatrix} \alpha^4 & \alpha & 1 & \alpha^4 \\ \alpha^3 & \alpha^{14} & \alpha & \alpha \\ \alpha^{14} & \alpha^3 & \alpha^4 & \alpha \\ \alpha & \alpha & \alpha^4 & 1 \end{bmatrix}$$ MDS matris, $\mathbb{F}_{2^4}/(0\times13)$ sonlu cismi üzerinde tanımlı

$\alpha^4, \alpha, 1, \alpha^3, \alpha^{14}$ elemanlarının, $\mathbb{F}_2$ cismi üzerinde 4×4 ikili matris karşılıkları

$$\alpha^4 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \alpha = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, 1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \alpha^3 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}, \alpha^{14} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

olmak üzere, A matrisinin $\mathbb{F}_2$ sonlu cismi üzerinde karşılığı olan 16×16 ikili matris Eşitlik (9.6)'da verilmiştir.

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \\ y_8 \\ y_9 \\ y_{10} \\ y_{11} \\ y_{12} \\ y_{13} \\ y_{14} \\ y_{15} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} . \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \\ x_{10} \\ x_{11} \\ x_{12} \\ x_{13} \\ x_{14} \\ x_{15} \end{bmatrix} \quad (9.6)$$

A matrisinin Eşitlik (9.6)'da verilen giriş $(x_0, x_1, \ldots x_{15})$ ve çıkış $(y_0, y_1, \ldots y_{15})$ haritalaması, cebirsel olarak Eşitlik (9.7)'deki gibi ifade edilebilir;

$$
\begin{aligned}
y_0 &= x_0 \oplus x_3 \oplus x_7 \oplus x_8 \oplus x_{12} \oplus x_{15} \\
y_1 &= x_0 \oplus x_1 \oplus x_3 \oplus x_4 \oplus x_7 \oplus x_9 \oplus x_{12} \oplus x_{13} \oplus x_{15} \\
y_2 &= x_1 \oplus x_2 \oplus x_5 \oplus x_{10} \oplus x_{13} \oplus x_{14} \\
y_3 &= x_2 \oplus x_3 \oplus x_6 \oplus x_{11} \oplus x_{14} \oplus x_{15} \\
y_4 &= x_1 \oplus x_4 \oplus x_5 \oplus x_{11} \oplus x_{15} \\
y_5 &= x_1 \oplus x_2 \oplus x_6 \oplus x_8 \oplus x_{11} \oplus x_{12} \oplus x_{15} \\
y_6 &= x_2 \oplus x_3 \oplus x_7 \oplus x_9 \oplus x_{13} \\
y_7 &= x_0 \oplus x_3 \oplus x_4 \oplus x_{10} \oplus x_{14} \\
y_8 &= x_0 \oplus x_1 \oplus x_5 \oplus x_8 \oplus x_{11} \oplus x_{15} \\
y_9 &= x_2 \oplus x_5 \oplus x_6 \oplus x_8 \oplus x_9 \oplus x_{11} \oplus x_{12} \oplus x_{15} \\
y_{10} &= x_3 \oplus x_6 \oplus x_7 \oplus x_9 \oplus x_{10} \oplus x_{13} \\
y_{11} &= x_0 \oplus x_4 \oplus x_7 \oplus x_{10} \oplus x_{11} \oplus x_{14} \\
y_{12} &= x_3 \oplus x_7 \oplus x_8 \oplus x_{11} \oplus x_{12} \\
y_{13} &= x_0 \oplus x_3 \oplus x_4 \oplus x_7 \oplus x_8 \oplus x_9 \oplus x_{11} \oplus x_{13} \\
y_{14} &= x_1 \oplus x_5 \oplus x_9 \oplus x_{10} \oplus x_{14} \\
y_{15} &= x_2 \oplus x_6 \oplus x_{10} \oplus x_{11} \oplus x_{15}
\end{aligned}
\tag{9.7}
$$

Tanım 9.12. (Derinlik): Devreyi oluşturan en uzun yolun uzunluğu olarak tanımlanabilir.

Bir yayılım matrisinde, devre derinliğinin minimum derinlikte olması ve bu devrenin minimum XOR sayısıyla gerçeklenmesi amaçlanır [24]. Bir devre farklı derinliklerle tasarlanabilir, literatürde yayılım tabakalarının devre derinliği optimizasyonu çalışılan açık problemlerden biridir [3].

Örnek 9.13: $v_1 = x_1 \oplus x_2 \oplus x_3 \oplus x_4$, $v_2 = x_5$, $v_3 = x_6 \oplus x_7 \oplus x_8 \oplus x_9$ olmak üzere $v_1 \oplus v_2 \oplus v_3$ toplam devresi farklı derinliklerde tasarlanabilir. Şekil 9.1 ve Şekil 9.2'de $v_1 \oplus v_2 \oplus v_3$ toplam devresinin farklı tasarımları verilmiştir. Şekiller üzerinde verilen kesik çizgiler "1 devre derinliğini" temsil etmektedir. Şekil 9.1 ve Şekil 9.2'de verilen toplam devreleri ve bu devreleri oluşturan alt devreler (ara değerler) ele alındığında v_1 alt devresinin derinliği; her iki tasarım için de 2'dir. v_2 alt devresinin derinliği her iki devre tasarımında da aynı olmak üzere 0'dır. Çünkü v_2 çıkış değeri x_5 giriş değerine eşit olup, v_2

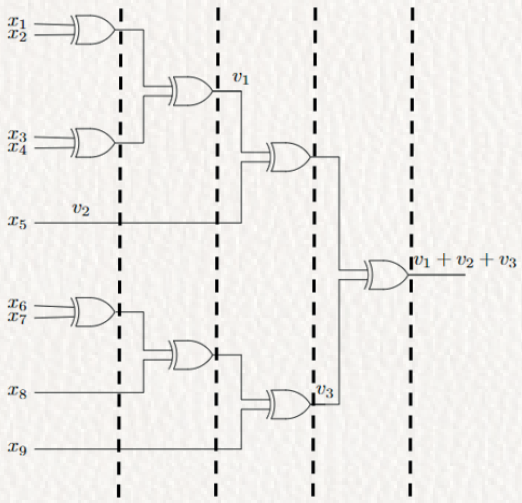
alt devresini oluşturmak için herhangi bir XOR kapısı kullanılmamıştır. v_3 alt devresinin derinliği her iki devre tasarımında da 3'tür. Ancak $v_1 \oplus v_2 \oplus v_3$ toplam devresinin derinlik değerleri ele alındığında;

$$v_1 \oplus v_2 \oplus v_3 = \left(\left(\underbrace{(x_1 \oplus x_2) \oplus (x_3 \oplus x_4)}_{v_1} \right) \oplus \underbrace{x_5}_{v_2} \right) \oplus \left(\underbrace{\left((x_6 \oplus x_7) \oplus x_8 \right) \oplus x_9}_{v_3} \right)$$ olarak

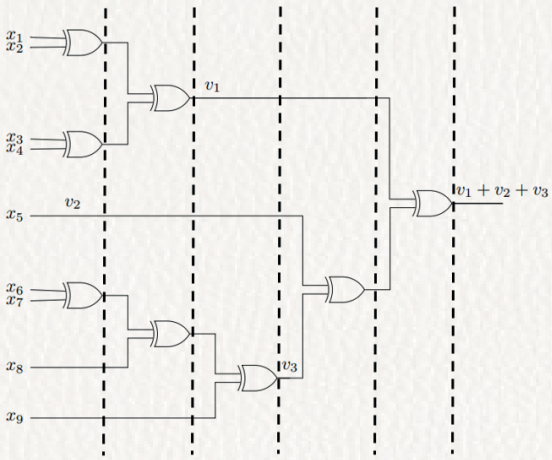
tasarlanan ve Şekil 9.1'de verilen $v_1 \oplus v_2 \oplus v_3$ toplam devresinin derinliği 4'tür.

$$v_1 \oplus v_2 \oplus v_3 = \left(\underbrace{(x_1 \oplus x_2) \oplus (x_3 \oplus x_4)}_{v_1} \right) \oplus \left(\underbrace{x_5}_{v_2} \oplus \left(\underbrace{\left((x_6 \oplus x_7) \oplus x_8 \right) \oplus x_9}_{v_3} \right) \right)$$ olarak

tasarlanan ve Şekil 9.2'de verilen $v_1 \oplus v_2 \oplus v_3$ toplam devresinin derinliği ise 5'tir.



Şekil 9.1. $(v_1 + v_2 + v_3)$ Devresinin 4 Derinlikli Tasarlanması



Şekil 9.2. $(v_1 + v_2 + v_3)$ Devresinin 5 Derinlikli Tasarlanması

Blok şifrelerde kullanılan yayılım matrisleri farklı devre tasarımları ile tasarlanabilir. En iyi devre tasarımının bulunması; devre derinliğinin azaltılmasının yanı sıra, matris devresinin giriş ve çıkış haritalamasının cebirsel ifadesini de değiştirir. Böylece cebirsel ifadenin daha az sayıda XOR sayısıyla ifade edilmesine imkân sağlar. Literatürde (tersi kendisine eşit) MDS matrislerin minimum derinlikte ve minimum XOR sayısıyla gerçeklenen devrelerle tasarlanması için, faklı optimizasyon yöntemleri önerilmiştir. Bölüm 9.4'te bu optimizasyon yöntemleri detaylarıyla verilmiştir.

Minimum XOR sayısı ve derinlik parametreleri ile düşük maliyetli (tersi kendisine eşit) MDS matrislerin tasarlanması hafif sıklet kriptosistemlerin yayılım tabakaları için son derece önemlidir. Bu nedenle Bölüm 9.3'te MDS matrisler için farklı tasarım yöntemleri ayrıntılı olarak ele alınmıştır.

9.3. (TERSİ KENDİSİNE EŞİT) MDS MATRİS TASARIM YÖNTEMLERİ

MDS matrisler diğer yayılım tabakalarına oranla maliyetlidir ancak en iyi yayılımı sağlarlar. Bu nedenle düşük maliyet ve düşük gecikmeli (tersi kendisine eşit) MDS matrislerin tasarımı önemli bir çalışma problemidir [29].

(Tersi kendisine eşit) MDS matrislerin tasarımı için iki temel tasarım yöntemi vardır; özyinelemeli (recursive) ve özyinelemeli–olmayan (non– recursive). Özyinelemeli tasarım yöntemleri seri–tabanlı (serial-based) uygulamalar olarak adlandırılırken, özyinelemeli–olmayan tasarım yöntemleri ise döngü–tabanlı (round–based) uygulamalar olarak adlandırılır. Özyinelemeli yapılarda matrisin k. kuvveti MDS matrisken, özyinelemeli–olmayan yapılarda ise matrisin kendisi MDS matristir [26].

Bunun yanında bir diğer (tersi kendisine eşit) MDS tasarım sınıflandırması ise; doğrudan tasarım (direct construction), arama (searching) ve hibrit (hybrid) yöntemlerle tasarım şeklinde yapılabilir. Bu sınıflandırma temelde bir matris formunun doğrudan MDS matris üretip üretmediği üzerine kurulmuştur [25], [26].

Tasarım yöntemleri aşağıda verilen alt başlıklarda kapsamlı olarak detaylandırılmıştır.

9.3.1. (Tersi Kendisine Eşit) MDS Matrisler için Özyinelemeli ve Özyinelemeli - Olmayan Tasarım Yöntemleri

Özyinelemeli yapılarda (tersi kendisine eşit) MDS matris, A seri matrisinin (genellikle Companion matrisle [26] başlar) k. kuvveti A^k olarak hesaplanır. A^k MDS matrisinin kendisinin devre uygulaması yerine, A matrisinin devresi k kez uygulanır. Yayılma özelliği MDS matris koşulundan dolayı maksimum kalırken, donanım maliyeti düşük kalır çünkü A matrisinin devresinin k kez uygulanması devre maliyetini çok arttırmaz [30].

Tanım 9.14. (Seri Matris): $z_0,\dots z_{d-1}\in\mathbb{F}_{2^m}$ olmak üzere $d\times d$ boyutlu $Seri(z_0,\dots z_{d-1})$ gösterimiyle seri matrisi Eşitlik (9.8)'deki gibidir;

$$Seri(z_0,\dots z_{d-1})=\begin{bmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 \\ z_0 & z_1 & \dots & \dots & \dots & z_{d-1} \end{bmatrix} \tag{9.8}$$

Böylece $Seri(z_0,\dots z_{d-1})^k$ matris formundan MDS matrisler üretilir.

Tanım 9.15. (Companion Matris):

$g(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{d-1}x^{k-1} + x^k \in \mathbb{F}_q[x]$ k. dereceden monik polinom (en yüksek dereceli terimin (x^k) katsayısı 1 olan polinom) olmak üzere, Companion matris C_g Eşitlik (9.9)'daki gibidir;

$$C_g = \begin{bmatrix} 0 & 1 & 0 & 0 & \ldots & 0 \\ 0 & 0 & 1 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & 0 & \ldots & 1 \\ -a_0 & -a_1 & \ldots & \ldots & \ldots & -a_{k-1} \end{bmatrix} \tag{9.9}$$

ve $Companion(-a_0, -a_1, \ldots, -a_{k-1})$ gösterimi ile ifade edilir.

Eşitlik (9.8)'de verilen $Seri(z_0, \ldots z_{d-1})$ matrisi aynı zamanda $z_0 + z_1x + z_2x^2 + \ldots z_{d-1}x^{d-1} + x^d$ polinomuna göre Companion matristir.

Özyinelemeli MDS matris tasarım yöntemlerinde seri matrislerin önemi açıktır. Bu nedenle literatürde daha düşük maliyetli seri matrislerin tasarımı için farklı formlar önerilmiştir. LFS (Linear Feedback Serial – Doğrusal Geribeslemeli Seri) matris formu [32] ve DSI (Diagonal – Serial Invertible – Diagonal Seri Tersi Alınabilir) matris formu [31] bu formlardan ikisidir. Bu matris formlarına ait tanımlar aşağıda verilmiştir.

Tanım 9.16. (LFS Matris): $L = LFS(z_0, z_1, \ldots, z_{k-1})$ matrisinin elemanları aşağıdaki gibi ifade edilir;

$$L_{ij} = \begin{cases} z_j, & i = k-1 \\ 1, & i+1 = j \\ 0, & diğer durumlarda \end{cases} \tag{9.10}$$

L matrisinin tersi L^{-1} matrisi aşağıdaki gibi ifade edilir;

$$L^{-1}_{ij} = \begin{cases} \dfrac{z_j + 1}{z_0}, & i = 0,\ z_k = 1 \\ 1, & i = j+1 \\ 0, & diğer durumlarda \end{cases} \tag{9.11}$$

Eşitlik (9.11)'deki ifade için eğer $z_0 = 1$ ise, LFS matrisin kendisi ve tersi aynı $z_1, z_2 \ldots, z_{k-1}$ sonlu cisim elemanlarına sahip olur. Diğer bir ifadeyle; her iki matris için gerekli donanım kaynağı birbirine eşittir [32]. Bunun yanında [31]'de verilen çalışmada $z_0 \neq 1$ olduğu durumlarda, kendisi ve tersi aynı donanım kaynaklarına sahip olan matrislerin varlığı ispatlanmıştır.

Tanım 9.17. (DSI Matris): $k \times k$ boyutlu $D = DSI(D_{ij})_{1 \le i,j \le k} \in \mathbb{F}_{2^n}$ matrisi $a = (a_i)_{1 \le i \le k} \in \mathbb{F}_{2^n}, a_i \neq 0$ ve $b = (b_i)_{1 \le i \le k-1} \in \mathbb{F}_{2^n}$ vektörleri tarafından belirlenir ve aşağıdaki gibi ifade edilir;

$$D_{ij} = \begin{cases} a_1, & i = 1, j = k \\ a_i, & i = j+1 \\ b_i, & i = j \le k-1 \\ 0, & diğer durumlarda \end{cases} \tag{9.12}$$

Örnek 9.18: 6×6 boyutlu $D_1 = DSI(a,b)$ matrisi aşağıdaki gibi ifade edilir;

$$D_1 = \begin{bmatrix} b_1 & 0 & 0 & 0 & 0 & a_1 \\ a_2 & b_2 & 0 & 0 & 0 & 0 \\ 0 & a_3 & b_3 & 0 & 0 & 0 \\ 0 & 0 & a_4 & b_4 & 0 & 0 \\ 0 & 0 & 0 & a_5 & b_5 & 0 \\ 0 & 0 & 0 & 0 & a_6 & 0 \end{bmatrix} \tag{9.13}$$

DSI matris formu $LFS(z_0, z_1, \ldots, z_{k-1})$ matris yapısından esinlenerek tasarlanmıştır. Tasarımdaki amaç; permütasyon matrisinin yapısı korunarak, satırların ikili doğrusal kombinasyonları ile daha yüksek yayılım sağlamaktır. DSI matrislerin cebirsel özellikleriyle ilgili kapsamlı bilgiye [31]'den erişilebilir.

Özyinelemeli yapılarda, DSI matrislerin kullanımı daha yüksek boyutlu matrisler için iyi sonuçlar elde edilmesini sağlasa da, DSI matrisler yerine Companion matrislerin kullanılması Companion matrislerin güçlü matematiksel teorisi nedeniyle kaçınılmazdır. Ancak arama yöntemiyle bulunabilecek küçük boyutlu matrisler için donanım maliyeti açısından kıyaslandığında; DSI matrisler Companion matrislere göre daha düşük maliyetli devreye sahip matrislerin üretilmesine imkân sağlar [26].

Özyinelemeli – olmayan yapılarda matrisin kendisi MDS matristir, seri matrislerdeki gibi matrisin k. kuvveti uygulanmaz. Cauchy ve Vandermonde matris formları bu yapıların üretilmesini sağlar, çünkü bu matris formları kanıtlanabilir MDS olma avantajına sahiptirler [33]. Bu matris formları Eşitlik (9.14) ve Eşitlik (9.15)'te verilmiştir.

Tanım 9.19. (Cauchy Matris): $k \times k$ boyutlu, $\{\alpha_0, \alpha_1, \ldots, \alpha_{k-1}\} \in \mathbb{F}_{2^n}$ ve $\{\beta_0, \beta_1, \ldots, \beta_{k-1}\} \in \mathbb{F}_{2^n}$ iki ayrık set, tüm $0 \le i, j \le n-1$ için $\alpha_i + \beta_i \neq 0$ olmak üzere, $C[i,j] = \dfrac{1}{\alpha_i + \beta_i}$ Cauchy matrisi aşağıdaki gibi ifade edilir;

$$C = \begin{bmatrix} \frac{1}{\alpha_0+\beta_0} & \frac{1}{\alpha_0+\beta_1} & \cdots & \frac{1}{\alpha_0+\beta_{k-1}} \\ \frac{1}{\alpha_1+\beta_0} & \frac{1}{\alpha_1+\beta_1} & \cdots & \frac{1}{\alpha_1+\beta_{k-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{\alpha_{k-1}+\beta_0} & \frac{1}{\alpha_{k-1}+\beta_1} & \cdots & \frac{1}{\alpha_{k-1}+\beta_{k-1}} \end{bmatrix} \tag{9.14}$$

Cauchy matrisler ile elde edilen katsayılar çok karmaşıktır, bu da donanım – verimli MDS matrislerin tasarlanmasına engeldir [34].

Tanım 9.20. (Vandermonde Matris): $n \times n$ boyutlu, $A = vand(a_0, a_1, \ldots a_{n-1})$ Vandermonde matrisi aşağıdaki gibi ifade edilir;

$$A = \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ a_0 & a_1 & a_2 & \ldots & a_{n-1} \\ a_0^2 & a_1^2 & a_2^2 & \ldots & a_{n-1}^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_0^{n-1} & a_1^{n-1} & a_2^{n-1} & \ldots & a_{n-1}^{n-1} \end{bmatrix} \tag{9.15}$$

Özyinelemeli ve özyinelemeli–olmayan yöntemler karşılaştırıldığında; özyinelemeli yapılar daha az donanım alanı gereksinimi için daha fazla saat vuruşuna (clock cycle) ihtiyaç duyar. Özyinelemeli – olmayan uygulamalarda

bir saat vuruşunda, $k \times k$ boyutu için yayılım matrisinin tümü hesaplanır ve uygulanır. Bu nedenle matrisin k^2 elemanının da olabildiğince düşük maliyetli (XOR sayılı) olması istenir. Özyinelemeli uygulamalarda seri matrisin önemsiz olmayan ($\neq 0$) satırı hesaplanır ve bu işlem k defa özyinelemeli olarak tekrarlanır. Bu nedenle hesaplama zamanı bir dizi k saat vuruşu alır.

9.3.2. (Tersi Kendisine Eşit) MDS Matrisler için Doğrudan Tasarım, Arama ve Hibrit Tasarım Yöntemleri

Doğrudan tasarım yöntemi, özel kodlar ve özel matris formları kullanılarak, üretilen matrisin doğrudan MDS matris olduğu yapılardır. Gabidulin [35] ve BCH [36] kodları cebirsel özellikleri sayesinde direkt olarak MDS matrislerin üretilmesini sağlar. Cauchy, Vandermonde ve Companion özel matris formlarının kullanılması ile de doğrudan MDS matrisler tasarlanabilir. Cauchy ve Vandermonde matris formları kullanılarak üretilen MDS matrisler donanım – verimli değildir, bu nedenle arama yöntemiyle üretilen MDS matrisler daha verimli uygulamalara sahiptir [26].

Arama yönteminde, rastgele üretim ve bazı özel matris formları kullanılarak bir matrisin MDS olup olmadığı kontrol edilir. Rastgele üretimde matrisin elemanları sonlu cisim üzerinden seçilerek, bu matrisin tüm alt kare matrislerinin tekil olmayan matris olup olmadığının kontrol edilmesi ve doğrulanması gerekir, böylece (tersi kendisine eşit) MDS matrislerin elde edilmesi sağlanır. Ancak aranacak uzay çok büyük olduğu için rastgele üretim yöntemi verimli bir yöntem değildir. Bu nedenle (tersi kendisine eşit) MDS matrislerin bulunması için; arama uzayı bazı özel matris formlarının kullanılmasıyla küçültülür. Cebirsel özellikleri sayesinde (tersi kendisine eşit) MDS matrislerin üretilmesini sağlayan bu özel matris formları aşağıdaki tanımlarda verilmiştir.

Tanım 9.21. (Dairesel Matris): $n \times n$ boyutlu, $A = Circ(a_0, a_1, \ldots a_{n-1})$ Dairesel (Circulant) matrisi aşağıdaki gibi ifade edilir;

$$A = \begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & \cdots & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{bmatrix} \tag{9.16}$$

Dairesel matrislerin yayılım tabakalarında kullanılmasının önemli avantajları vardır [26];

- Dairesel matris formuyla MDS matrislerin bulunma olasılığı, rastgele üretim yöntemiyle kıyaslandığında yüksektir,
- $n \times n$ boyutlu Cauchy ve Hadamard matris formundaki matrislerin MDS matris olabilmeleri için; en az n farklı elemana sahip olmaları gerekirken, Dairesel matris formunda ise en çok n farklı eleman kullanılır. Bu da daha düşük donanım maliyetli MDS matrislerin üretilmesini sağlar,
- Dairesel matris formu özyinelemeli ve özyinelemeli – olmayan MDS matris tasarımlarının ikisinde de kullanılır.
- Dairesel matrisler avantajlarının yanı sıra bazı dezavantajlara da sahiptir [37];
- Dairesel MDS matrisler ile tersi kendisine eşit MDS matrisler üretilemez,
- $2^n \times 2^n$ Dairesel MDS matrisler ortogonal değildir.

Bu nedenle tersi kendisine eşit MDS matrislerin bulunması için sol – Dairesel matris formu önerilmiştir. Bu formda, her satır vektörü bir önceki satır vektörünün bir eleman dairesel sola kaydırılmasıyla elde edilir.

Tanım 9.22. (sol – Dairesel Matris): $n \times n$ boyutlu, $B = l - Circ(a_0, a_1, \ldots a_{n-1})$ sol – Dairesel (left–Circulant) matrisi aşağıdaki gibi ifade edilir;

$$B = \begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_1 & a_2 & a_3 & \cdots & a_0 \\ a_2 & a_3 & a_4 & \cdots & a_1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \end{bmatrix} \tag{9.17}$$

Daha verimli MDS matrislerin tasarımı için Dairesel – benzeri (Circulant–like) matris formu [38] önerilmiştir. [37]'de verilen çalışmada Dairesel–benzeri matris formu ele alınarak, Tip–I Dairesel–benzeri (Type–I Circulant–like) ve Tip–II Dairesel – benzeri (Type-II Circulant–like) matris formları önerilmiştir.

Tanım 9.23. (Tip – I Dairesel – benzeri Matris): $A = Circ(1, a_1, \ldots, a_{n-2})$, $\mathbf{1} = \underbrace{(1,1,\ldots,1)}_{n-1 \text{ tane}}$ ve $\mathbf{1}$ birim eleman, $a \neq 0, a_i \neq 0, i = \{1,2,\ldots(n-2)\}$ olmak üzere, $n \times n$ boyutlu, Tip – I Dairesel – benzeri matris $T_1 = TypeI\left(a, Circ(1, a_1, \ldots, a_{n-2})\right)$ aşağıdaki gibi ifade edilir;

$$T_1 = \begin{bmatrix} a & \mathbf{1} \\ \mathbf{1}^T & A \end{bmatrix} \tag{9.18}$$

Tip-I Dairesel-benzeri matris formunun tersi neredeyse kendisine eşittir, bu form Neredeyse Tip–I Dairesel–benzeri (Almost Type–I Circulant–like) olarak adlandırılmış olup matris formu Eşitlik (9.19)'da verilmiştir.

Tanım 9.24. (Neredeyse Tip – I Dairesel – benzeri Matris): $A = Circ(a_0, \ldots, a_{n-2})$, $\mathbf{b} = \underbrace{(b,b,\ldots,b)}_{n-1 \text{ tane}}$, $a, b \neq 0, a_i \neq 0, i = \{0,1,\ldots(n-2)\}$ olmak üzere, $n \times n$ boyutlu, Neredeyse Tip–I Dairesel–benzeri matris $T_2 = AlmostTypeI\left(a, b, Circ(a_0, \ldots, a_{n-2})\right)$ aşağıdaki gibi ifade edilir;

$$T_2 = \begin{bmatrix} a & \mathbf{b} \\ \mathbf{b}^T & A \end{bmatrix} \tag{9.19}$$

Tip–I Dairesel–benzeri matris formu çift boyutlarda tersi kendisine eşit MDS veya ortogonal MDS matrisler üretmez, bu nedenle Tip–II Dairesel–benzeri matris formu önerilmiştir.

Tanım 9.25. (Tip–II Dairesel–benzeri Matris): $A = Circ(a_0, \ldots, a_{n-1})$ olmak üzere, $2n \times 2n$ boyutlu Tip–II Dairesel–benzeri matris $T_3 = TypeII\left(Circ(a_0, \ldots, a_{n-1})\right)$ aşağıdaki gibi ifade edilir;

$$T_3 = \begin{bmatrix} A & A^{-1} \\ A^3 + A & A \end{bmatrix} \tag{9.20}$$

n tek sayı olmak üzere $2n \times 2n$ boyutlu Tip–II Dairesel–benzeri matris formu tersi kendisine eşit MDS matrislerin üretilmesini sağlar [37].

Tanım 9.26. (Toeplitz Matris): $n \times n$ boyutlu Toeplitz matris $T_4 = Toep(a_0, a_1 \ldots, a_{n-1}; a_{-1}, a_{-2}, \ldots, a_{-(n-1)})$ aşağıdaki gibi ifade edilir;

$$T_4 = \begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-2} & a_{n-1} \\ a_{-1} & a_0 & a_1 & \cdots & a_{n-3} & a_{n-2} \\ a_{-2} & a_{-1} & a_0 & \cdots & a_{n-4} & a_{n-3} \\ a_{-3} & a_{-2} & a_{-1} & \cdots & a_{n-5} & a_{n-4} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{-(n-1)} & a_{-(n-2)} & a_{-(n-3)} & \cdots & a_{-1} & a_0 \end{bmatrix} \tag{9.21}$$

Dairesel matrisler Toeplitz matrislerin özel bir formudur. Toeplitz matris formunda; soldan sağa azalan köşegen üzerindeki elemanlar sabittir. Toeplitz matris formunun gösterimi; matrisin birinci satır ve birinci sütun elemanları yan yana yazılarak ifade edilir;

$$Toep(\underbrace{a_0, a_1 \ldots, a_{n-1}}_{\text{birinci satır elemanları}}; \underbrace{a_{-1}, a_{-2}, \ldots, a_{-(n-1)}}_{\text{birinci sütun elemanları}}).$$

Elemanları $\mathbb{F}_{2^n}$ üzerinde tanımlı, $k \geq 3$ olmak üzere $k \times k$ boyutlu bir Toeplitz MDS matrisin tersi kendisine eşit olamaz. Ayrıca $k \geq 2$ olmak üzere $2^k \times 2^k$ boyutlu Toeplitz matris ortogonal ise, bu matris MDS matris olamaz [26].

Tanım 9.27. (Hankel Matris): $n \times n$ boyutlu Hankel matris $H = Hank(a_0, a_1 \ldots, a_{n-1}; a_n, a_{n+1}, \ldots, a_{2n-2})$ aşağıdaki gibi ifade edilir;

$$H = \begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-2} & a_{n-1} \\ a_1 & a_2 & a_3 & \cdots & a_{n-1} & a_n \\ a_2 & a_3 & a_4 & \cdots & a_n & a_{n+1} \\ a_3 & a_4 & a_5 & \cdots & a_{n+1} & a_{n+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-1} & a_n & a_{n+1} & \cdots & a_{2n-3} & a_{2n-2} \end{bmatrix} \tag{9.22}$$

Hankel matris, Toeplitz matris formunun satır permütasyonu uygulanmış hâlidir. Aynı zamanda sol – Dairesel matris formunun özel bir durumudur. Hankel matris cebirsel olarak Toeplitz matrisin özelliklerini gösterir. Şöyle ki; elemanları $\mathbb{F}_{2^n}$ üzerinde tanımlı, $k \geq 3$ olmak üzere $k \times k$ boyutlu bir Hankel MDS matrisin tersi kendisine eşit olamaz. Ayrıca, $k \geq 2$ olmak üzere $2^k \times 2^k$ boyutlu Hankel matris ortogonal ise, bu matris MDS matris olamaz [26].

Tanım 9.28. (Hadamard Matris): Elemanları $\mathbb{F}_{2^m}$ üzerinde tanımlı, $2^k \times 2^k$ boyutlu sonlu cisim Hadamard (finite field Hadamard – kısaca Hadamard) matris H aşağıdaki gibi ifade edilir;

$$H = \begin{bmatrix} U & V \\ V & U \end{bmatrix} \tag{9.23}$$

U **ve** V alt matrisleri de Hadamard matristir. 4×4 boyutlu $H_1 = Had(a_0, a_1, a_2, a_3)$ Hadamard matrisi Eşitlik (9.24)'te verilmiştir.

$$H_1 = \begin{bmatrix} a_0 & a_1 & a_2 & a_3 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_3 & a_0 & a_1 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix} \tag{9.24}$$

Bir Hadamard matrisin eğer ilk satırındaki elemanların toplamı 1'e eşitse bu matrisin tersi kendisine eşittir [39]. Elemanları $\mathbb{F}_{2^m}$ üzerinde tanımlı $k \times k$ boyutlu Hadamard matrislere ait önemli özellikler aşağıda verilmiştir [40];

- $k \times k$ boyutlu H Hadamard matrisinin, a_i ilk satır elemanlarını temsil etmek üzere, $H_{i,j} = a_{i \oplus j}$'dir.
- $k \times k$ boyutlu H Hadamard matrisi bi-simetrik matristir. Şöyle ki; $H = H^T$ ve $HJ = JH$ (J matrisi $k \times k$ boyutlu dönüşüm (exchange) matrisi olmak üzere, yani $J_{i,k-i+1} = 1$, diğer elemanları ise 0'dır).
- $c = \bigoplus_{i=0}^{k-1} a_i$ ve I $k \times k$ boyutlu birim matris olmak üzere, $H^2 = c^2 I$ koşulunu sağlar.

Hadamard matrisler, iki Vandermonde matris kullanılarak üretilebildiği gibi [41], Cauchy matrisler kullanılarak da üretilebilir ve bu matris formu Hadamard-Cauchy olarak adlandırılır [23].

MDS matrislerin üretilmesi için birçok farklı özel matris formundan yararlanılırken, tersi kendisine eşit MDS matrislerin üretilmesi için bilinen yöntemler; rastgele üretim yöntemi, Hadamard matris formu, Tip–II Dairesel–benzeri matris formudur. Bu nedenle özellikle tersi kendisine eşit MDS matrislerin üretilmesi için hibrit üretim yöntemi önerilmiştir.

Hibrit üretim yöntemi GHadamard (Generalized Hadamard – Genelleştirilmiş Hadamard) [40] matris formunun önerilmesiyle ortaya çıkmıştır. Hibrit yöntemde, (tersi kendisine eşit) MDS matrislerin arama maliyetini düşürmek için doğrudan üretim ve arama yöntemleri birleştirilmiştir. Hibrit yapı, temeline özel matris formlarını alır ve bu özel matris formları kullanılarak yeni (tersi kendisine eşit) MDS matrisler arama maliyeti olmadan doğrudan üretilir. Arama yöntemi doğrudan üretilen (tersi kendisine eşit) MDS matrisler içinden minimum XOR sayılı matrislerin bulunması için kullanılır. GHadamard matris formu, tersi kendisine eşit MDS matrislerin üretilmesini sağlayan kısıtlı üretim yöntemlerinden biridir.

Tanım 9.29. (GHadamard Matris): Elemanları $\mathbb{F}_{2^m}$ üzerinde tanımlı, 2×2 boyutlu $H = Had(a_0, a_1)$ Hadamard matrisi, $b_1 \neq 0, b_1 \in \mathbb{F}_{2^n}$ olmak üzere, 2×2 boyutlu $GH = Ghad(a_0, a_1; b_1)$ GHadamard matrisi aşağıdaki gibi ifade edilir;

$$GH = \begin{bmatrix} a_0 & a_1 b_1 \\ a_1 b_1^{-1} & a_0 \end{bmatrix} \tag{9.25}$$

4×4 boyutlu $GH_1 = Ghad(a_0, a_1; b_1, a_2; b_2, a_3; b_3)$ GHadamard matrisi Eşitlik (9.26)'da verilmiştir.

$$GH_1 = \begin{bmatrix} a_0 & a_1 b_1 & a_2 b_2 & a_3 b_3 \\ a_1 b_1^{-1} & a_0 & a_3 b_1^{-1} b_2 & a_2 b_1^{-1} b_3 \\ a_2 b_2^{-1} & a_3 b_2^{-1} b_1 & a_0 & a_1 b_2^{-1} b_3 \\ a_3 b_3^{-1} & a_2 b_3^{-1} b_1 & a_1 b_3^{-1} b_2 & a_0 \end{bmatrix} \tag{9.26}$$

GHadamard matris formu; verilen Hadamard tersi kendisine eşit MDS matristen yeni tersi kendisine eşit MDS matrislerin doğrudan üretilmesini sağlarken, Hadamard MDS matrislerden de yeni Hadamard MDS matrisler üretir. GHadamard matris formu tek veya çift herhangi bir boyuta uygulanabilir, bu da Tip – II Dairesel – benzeri matris formundaki gibi kısıtlamaya sebep olmaz.

Tanım 9.30. Elemanları $\mathbb{F}_{2^m}$ üzerinde tanımlı $A=\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$ matrisi eğer tersi kendisine eşitse, A matrisi a_{11}, a_{22} elemanları ile ifade edilebilir, şöyle ki $a_{11} \neq a_{22} \neq a_{33}$ ve $b_0, b_1 \in \mathbb{F}_{2^m} - \{0\}$ olmak üzere $a_{12}=(a_{11}+1)b_0$, $a_{13}=(a_{11}+1)b_1$, $a_{21}=(a_{22}+1)b_0^{-1}$, $a_{23}=(a_{22}+1)b_0^{-1}b_1$, $a_{31}=(a_{11}+a_{22})b_1^{-1}$, $a_{32}=(a_{11}+a_{22})b_1^{-1}b_0$, $a_{33}=a_{11}+a_{22}+1$ olur. Buradan 3×3 boyutlu tersi kendisine eşit matris formu $(IM)_{3x3}$ aşağıdaki gibi ifade edilir;

$$(IM)_{3X3}=\begin{bmatrix} a_{11} & (a_{11}+1)b_0 & (a_{11}+1)b_1 \\ (a_{22}+1)b_0^{-1} & a_{22} & (a_{22}+1)b_0^{-1}b_1 \\ (a_{11}+a_{22})b_1^{-1} & (a_{11}+a_{22})b_1^{-1}b_0 & a_{11}+a_{22}+1 \end{bmatrix} \quad (9.27)$$

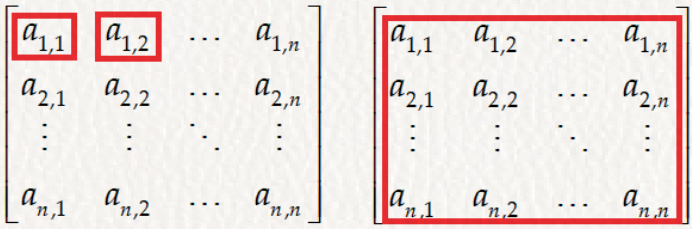
Eşitlik (9.27)'de verilen $(IM)_{3x3}$ matris formu üzerinde $a_{11} \neq a_{22}$, $a_{11}, a_{22} \neq 0$, $a_{11}, a_{22} \neq 1$, $a_{11}+a_{22} \neq 1$ ve $b_0, b_1 \in \mathbb{F}_{2^m} - \{0\}$ kısıtları altında, bu matris formu ile $\mathbb{F}_{2^m}$ üzerinde 3×3 boyutlu tersi kendisine eşit MDS matrislerin tamamı üretilebilir [54].

(Tersi kendisine eşit) MDS matrisler farklı üretim yöntemleriyle tasarlanırken bir taraftan da minimum XOR sayılı ve minimum derinlikli matrislerin bulunması için optimizasyon yöntemleri önerilmiştir. Bölüm 9.4'te bu yöntemler verilmiştir.

9.4. (TERSİ KENDİSİNE EŞİT) MDS MATRİSLER İÇİN YEREL VE GENEL OPTİMİZASYON YÖNTEMLERİ

Bir blok şifrenin yayılım tabakasında kullanılmak üzere (tersi kendisine eşit) MDS matrisler tasarlanırken bu matrisin özellikle donanım maliyetinin minimum olması beklenir ve bunun için farklı optimizasyon yöntemleri önerilmiştir. Bu yöntemler temelde; yerel optimizasyon (local optimization) ve genel

optimizasyon (global optimization) olarak ikiye ayrılır. Şekil 9.3'te yerel (a) ve genel (b) optimizasyon yöntemleri arasındaki fark bir yayılım matrisi üzerinde gösterilmiştir. Yerel optimizasyon yöntemlerinde; matrisin elemanlarına ayrı ayrı odaklanılarak bu elemanların minimum XOR sayılı elemanlardan seçilmesi hedeflenir. Genel optimizasyon (global optimization) yöntemlerinde ise matrisin tamamına odaklanılarak tüm yayılım matrisinin XOR sayısı optimize edilir.



Şekil 9.3. a) Yerel Optimizasyon b) Genel Optimizasyon

Literatürde yer alan yerel ve genel optimizasyon yöntemleri aşağıdaki alt başlıklarda kapsamlı olarak verilmiştir.

9.4.1. (Tersi Kendisine Eşit) MDS Matrisler için Yerel Optimizasyon Yöntemleri

Özyinelemeli yapılarla üretilen MDS matrislerin yerel optimizasyonu ele alındığında, bu yöntemler en genel ifadeyle özyinelemeli seri matristen üretilen MDS matrislerin elemanlarına odaklanarak verimli matrislerin üretilmesini hedefler. "Yayılım matrislerinin donanım uygulamalarında devre alanının azaltılması" fikri, 2007 yılında PRESENT şifreleme algoritmasının yayılım tabakasında özyinelemeli matrislerin kullanımıyla ortaya atılmıştır. Şifreleme algoritmalarının yayılım tabakalarında özyinelemeli seri matrislerin uygulanması fikri yeni bir araştırma alanını açmıştır. 2011 yılında LED blok şifreleme algoritması ve PHOTON hash fonksiyonunun [42] yayılım tabakalarında da seri matrislerle oluşturulan MDS matrisler kullanılmıştır. Sonraki yıllarda yapılan çalışmalarda "verimli MDS matrislerin oluşturulabilmesi için, seri mat-

risin elemanları nasıl seçilmelidir" sorusu üzerine yoğunlaşılmıştır. 2012 yılında yapılan çalışmada [41], farklı matris boyutları için farklı formlara sahip yayılım matrisleriyle en iyi yayılmanın sağlanabilmesi için, daha az sayıda doğrusal fonksiyonun kullanılması fikri önerilmiştir. 2013 yılında yapılan çalışmada [43], en iyi yayılım tabakalarının üretilmesi için iterasyon sayısı arttırılarak bit–seviyeli LFSR'lerin (Linear Feedback Serial Register–Doğrusal Geri-beslemeli Seri Yazmaç) kullanılması fikri ortaya atılmıştır. 2015 yılında yapılan çalışmada [44], düşük maliyetli tersi kendisine eşit MDS matrislerin üretilmesi için LFSR'lerden üretilen yayılım tabakalarına odaklanılmıştır. Aynı yıl yapılan bir diğer çalışmada ise [36], özyinelemeli MDS matrislerin doğrudan üretimi için BCH kodlar kullanılmıştır. 2017 yılında yapılan çalışmada [45], özyinelemeli MDS matrislerin üretilmesi için kullanılabilecek farklı BCH kod sınıf adayları verilmiştir. Bu sınıflar sayesinde; arama uzayı küçültülerek arama karmaşıklığı düşürülmüştür. Ayrıca, özyinelemeli yapılarla MDS matris üretimi için Companion matrislerin kullanılması verimli uygulamaların elde edilmesini sağlamıştır. Özyinelemeli yapılarla üretilen (tersi kendisine eşit) MDS matrisler için önerilen yerel optimizasyon yöntemleri ele alındığında, bu alanın iyi çalışıldığı ve çalışmaların doyum noktasına ulaştığı görülebilir [36].

Özyinelemeli – olmayan döngü – tabanlı MDS matrislerin donanım uygulamaları, özyinelemeli seri matrislere oranla daha verimlidir [39]. Bu nedenle özellikle XOR sayısı metriği tanıtıldıktan sonra çalışmalar, "döngü – tabanlı MDS matrislerin minimum XOR sayılı yerel optimizasyon uygulamalarının bulunması" üzerine odaklanmıştır. Başlangıçta bir yayılım matrisinin ikili matris gösterimindeki 1'lerin sayısı, bu matrisin donanım uygulaması için gereken XOR sayısı değeri için sınır değer olarak kullanılmıştır ancak bu sınır değeri ilgili yayılım matrisi için gereken maksimum XOR sayısının sınır değeridir. Bu nedenle sonraki çalışmalarda maksimum sınır değerinin "yayılım matrisinin elemanlarına odaklanılarak (diğer bir ifadeyle minimum XOR sayılı elemanları seçerek)" düşürüleceği gösterilmiştir [24]. 2015 yılında yapılan çalışmada [39], donanım – verimli MDS matrislerin tasarımı için indirgenemez polinom seçiminin önemli olduğu kanıtlanmıştır. Çünkü bir eleman, farklı indirgenemez polinomlarla üretilen sonlu cisimler üzerinde, farklı XOR

sayılarına sahiptir. Aynı çalışmada minimum XOR sayılı tersi kendisine eşit MDS matrislerin bulunması için, Hadamard – Cauchy formunda matrisler önerilmiştir. 2016 yılında yapılan çalışmada [30], farklı sonlu cisimler üzerinde her bir eleman için gereken XOR sayıları verilerek, optimum XOR sayısına sahip elemanlarla oluşturulan tersi kendisine eşit MDS matrisler verilmiştir. 2017 yılında yapılan çalışmada [46], Toeplitz matrisler kullanılarak minimum XOR sayılı MDS matrisler üretilmiştir. Elemanları F_{2^n} sonlu cismi üzerinde tanımlı (tersi kendisine eşit) MDS matrisin, F_2 sonlu cismi üzerinde $n \times n$ blok matrisle ifade edilebileceği Örnek 9.11'de verilmiştir. 2018 yılında yapılan çalışmada [47], bu gösterim (blok matrisle ifade etme) kullanılarak yapılan arama veya üretim yöntemlerinde bazı (tersi kendisine eşit) MDS matrislerin bulunamayacağı problemi ele alınmıştır. Çünkü F_2 sonlu cismi üzerinde her matris F_{2^n} sonlu cismi üzerinde temsil edilmeyebilir, bu durum minimal polinomun indirgenemez olup olmadığına bağlıdır. Çalışmada ayrıca blok Vandermonde ve blok Cauchy – benzeri matrisler kullanarak (tersi kendisine eşit) MDS matrisler doğrudan üretilmiştir. 2018 yılında yapılan çalışmada [40], GHadamard matris formuyla farklı boyutlarda ve farklı indirgenemez polinom altında minimum XOR sayılı (tersi kendisine eşit) MDS matrisler verilmiştir. 2019 yılında yapılan çalışmada [54], F_{2^n} sonlu cismi üzerinde 3×3 boyutlu tersi kendisine eşit MDS matrislerin tamamının üretildiği yeni bir matris formu önerilmiştir. 2020 yılında yapılan çalışmada [55] ise, MDS matrislerin otomorfizma ve izomorfizmaları tanımlanarak, bu matrislerin verimli uygulamaları elde edilmiştir.

Özyinelemeli – olmayan yapılarla üretilen (tersi kendisine eşit) MDS matrisler için önerilen yerel optimizasyon yöntemleri ele alındığında, bu yöntemlerle sadece matrisin elemanlarına odaklanıldığı açıkça görülebilir. Ancak 2017 yılında Kranz ve arkadaşlarının, verilen bir yayılım matrisinin elemanlarının yerel optimizasyonu yerine, matrisin tamamına odaklanıp genel optimizasyon yöntemleriyle daha düşük XOR sayılı matrisler elde edilebileceğini göstermeleriyle, çalışmaların neredeyse tamamı genel optimizasyon yöntemleriyle (tersi kendisine eşit) MDS matrislerin bulunması üzerine kaymıştır [33].

9.4.2. (Tersi Kendisine Eşit) MDS Matrisler için Genel Optimizasyon Yöntemleri

Temelde, genel optimizasyon yöntemlerinde yayılım matrisini oluşturan doğrusal fonksiyonların devresi, Doğrusal Düz Sıralı Program (Linear Straight - Line Programs) olarak ifade edilir. Bu sıralı programlar $X_i = X_j \oplus X_k$ formundaki talimatlarla gerçekleştirilir, burada X_i programda daha önce görülmeyen bir toplam ifadesiyken, X_j ve X_k programda daha önce görülen girdileri ifade eder [48]. Genel optimizasyon yöntemlerinde amaç, bir yayılım matrisinin devresini uygulayabilecek en kısa doğrusal programı (Shortest Linear Program - SLP) bulmaktır. En kısa SLP programı minimum derinlik ve minimum XOR sayısıyla devrenin tasarımını verir. Burada matrisin elemanlarına değil, matrisi oluşturan devrenin tamamı göz önünde bulundurulur.

İki farklı genel optimizasyon tekniği vardır; iptalsiz (cancellation – free) programlar ve sezgisel (heuristic) yöntemler. İptalsiz programlarda, $u = v \oplus w$ programının her satırı için, v değişkenlerinin hiçbiri w ifadesinde mevcut değildir, yani hesaplamada değişkenlerin iptali yoktur ve program iptale izin vermeyecek şekilde tasarlanır. Şöyle ki; $v = x_1 + x_2, w = x_1 + x_3$ ise program $v \oplus w$ işlemine izin vermeyecektir çünkü her iki değişken de x_1 girdisini içerdiğinden x_1 girdileri birbirini iptal edecektir. Bu nedenle iptalsiz programlarda bu duruma yol açacak değişkenlerin toplamlarına izin verilmez. Sezgisel optimizasyon yöntemleri ise iptallere izin vererek genel (common) optimum devre yolunun bulunması için önerilen programlardır.

Paar 1997 yılındaki çalışmasında [49], $\mathbb{F}_{2^n}$ sonlu cismi üzerinde sabit bir elemanla çarpma işlemi için gereken XOR sayısının Red – Solomon kodlayıcıları kullanarak azaltılabileceğini göstermiştir. Aynı çalışmada PAAR1 ve PAAR2 genel optimizasyon algoritmalarını önermiştir. Bu algoritmalar iptale izin vermezler bu nedenle iptalsiz programlardır. Her iki algoritma temelde en çok geçen alt ifadelerin bulunmasına ve bu ifadelerin toplanmasına dayanır. PAAR2 algoritmasının PAAR1'den farkı, işlemleri iteratif olarak yapmasıdır. Çalışmada $\mathbb{F}_{2^4}$ sonlu cismi üzerinde %17.5, $\mathbb{F}_{2^8}$ sonlu cismi üzerinde %40 XOR sayılarında azalma sağlanmıştır.

Örnek 9.31 : $\begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$ yayılım matrisinin PAAR1 algoritması kullanılarak genel optimizasyonu yapıldığında;

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix} \rightarrow \begin{matrix} x_0 \oplus x_2 \oplus x_3 \\ x_0 \oplus x_1 \oplus x_2 \\ x_0 \oplus x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{matrix} \tag{9.28}$$

Başlangıçta en çok geçen alt ifadeler belirlenir; $(x_0 \oplus x_2)$, daha sonra t_0 ara değişkenine $t_0 = x_0 \oplus x_2$ değeri verilir ve cebirsel ifade aşağıdaki gibi ifade edilir;

$$\rightarrow \begin{matrix} t_0 \oplus x_3 \\ t_0 \oplus x_1 \\ t_0 \oplus x_1 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{matrix} \tag{9.29}$$

Sonrasında yine en çok geçen alt ifadeler belirlenir; $(t_0 \oplus x_1)$, daha sonra t_1 ara değişkenine $t_1 = t_0 \oplus x_1$ değeri verilir ve cebirsel ifade aşağıdaki gibi ifade edilir;

$$\rightarrow \begin{matrix} t_0 \oplus x_3 \\ t_1 \\ t_1 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{matrix} \tag{9.30}$$

Genel optimizasyon yapılmadan önce Eşitlik (9.28)'de verilen yayılım matrisi 9 XOR sayısıyla uygulanabilirken, PAAR1 genel optimizasyon algoritmasının uygulanmasıyla Eşitlik (9.30)'dan da görüleceği gibi 4 XOR sayısıyla uygulanabilir.

Boyar ve Peralta 2010 yılındaki çalışmasında [50], yeni bir sezgisel optimizasyon yöntemi önermiştir. Hangi alt ifadelerin birbiriyle toplanacağına karar verilirken yeni mesafelerin toplamını minimum yapan çiftler seçilir, seçim sonucunda eğer kuyruk oluşursa (mesafe değerleri birbirine eşitse) öklid normu (normu maksimum yapan çiftler seçilir) kullanılır. Önerilen yöntem PAAR1 algoritmasından yavaştır ancak XOR sayılarında iyileşmeler sağlamıştır. Boyar ve arkadaşları 2013 yılındaki çalışmalarında [51] ise SLP programları geliştirerek, [50]'deki çalışmada verilen sonuçları daha da optimize etmişlerdir. Boyar ve arkadaşlarının 2017 yılındaki çalışmasında [52], gerekli maksimum derinlik değeri korunarak, PAAR1 ve PAAR2 algoritmaları ön işleme adımları eklenerek ve iptallere izin verilerek iyileştirilmiştir. Önerilen yöntemde devre üzerinde şu adımlar uygulanır; doğrusal olmayan bileşenlerin daha düşük derinlikli yapılara yeniden sentezlenmesi, önerdikleri See-Saw Yöntemi ile doğrusal bileşenleri yeniden sentezleyen rastgele açgözlü (greedy) bir sezgisel yöntem uygulanması. Bu yöntem sayesinde global optimizasyon için verimli sonuçlar elde edilmiştir. Boyar ve arkadaşlarının 2019 yılındaki çalışmasında [53] ise, verilen derinlik sınırı değerine göre küçük devrelerin oluşturulması için yeni bir sezgisel DCLO (Depth - Constrained Linear Optimization – Derinlik Sınırlı Doğrusal Optimizasyon) yöntemi önerilmiştir. Yöntem [52]'de verilen See-Saw algoritmasını iteratif olarak tekrarlayarak kullanır.

Tan ve Peyrin 2019 yılındaki çalışmasında [3], [50]'de verilen optimizasyon yöntemine rastgelelik ekleyerek RNBP (Random Normal Boyar Peralta) algoritmasını önermişlerdir. Çalışmada ayrıca deterministik olmayan A1 ve A2 optimizasyon algoritmaları da önerilmiştir. Bu algoritmalar da RNBP gibi [50]'de verilen algoritma tabanlıdır. Ancak bu algoritmaların temel farkı, olabildiğince çok sayıda yakın hedefin mesafesini azaltabilecek elemanın aranması yerine, en yakın hedeflerden biri seçilerek bu hedefi minimum yapacak kapı (girdi çiftleri) seçilir. Bu adım filtreleme (filtering) adımı olarak adlandırılmıştır. Filtreleme adımı daha uzaktaki hedefleri en aza indirgeyen kapıları filtrelemek için kullanılır, böylece bu kapılarla işlem yapılmaz. Filtreleme işleminden sonra toplam mesafeyi minimum yapan kapılardan birinin seçildiği seçme (selection) adımı uygulanır. Sonrasında kuyruğun kırılması işlemi [50]'deki gibi öklid normunu maksimum yapan çiftlerin seçileceği kuyruk–kırma (tie–breaking) adımı uygulanır. Son adım olan rastgeleleştirme (randomisation) adımında ise, eğer kuyruk – kırma adımı kuyruğu kırmak için çözüm sağlamazsa aday kapılar arasından rastgele biri seçilir. A2 algoritma-

sında A1 algoritmasından farklı olarak, kuyruk – kırma adımı atlanır böylece daha fazla rastgelelik sağlanmış olur.

Tablo 9.1'de yukarı verilen genel optimizasyon yöntemlerinin özet bir karşılaştırılması verilmiştir.

Tablo 9.1. Genel Optimizasyon Yöntemlerinin Karşılaştırılması

Algoritma	Yıl	Yöntem	Dezavantajları
PAAR1 (iptalsiz) [49]	1997	İteratif olarak alt ifadeleri eler.	En sık geçen çiftler önceden hesaplanabilir bu da sadece yerel optimum çözüm sağlar, genel optimum çözüm garanti etmez.
PAAR2 (iptalsiz) [49]	1997	İteratif olarak alt ifadeleri eler. En yüksek frekans değerine sahip tüm olası çiftleri kontrol eder.	En sık geçen çiftler önceden hesaplanabilir bu da sadece yerel optimum çözüm sağlar, genel optimum çözüm garanti etmez.
BP10 (sezgisel) [50]	2010	İptallere izin verir. İki adımdan oluşur; ilk adımda doğrusal olmayan bileşenler (AND kapısı) optimize edilirken, ikinci adımda doğrusal bileşenler (XOR kapısı) optimize edilir.	Devre derinliğini önemsemez.
BP13 (sezgisel) [51]	2013	BP10 ile çok benzerdir. Yöntem iptallere izin verir. İki adımdan oluşur; ilk adımda doğrusal olmayan bileşenler (AND kapısı) ad – hoc sezgisel yöntemiyle optimize edilirken, ikinci adımda doğrusal bileşenler (XOR kapısı) optimize edilir. Eğer kuyruk oluşursa öklid norm değerini maksimum yapan çiftler seçilir.	Devre derinliğini önemsemez.
BP17 (sezgisel) [52]	2017	BP10 ve BP13 ile çok benzerdir. Daha düşük derinlikli devreler bulmak için See-Saw metodu uygulanır.	Devre derinliği önemsenir ancak verilen devre derinliği sınır değerine göre kısıtlama yapılamaz.
BP19 (sezgisel) [53]	2019	Verilen devre derinliğine göre küçük doğrusal devrelerin bulunması için DCLO yöntemini kullanır. Doğrusal bileşenlerin alt ve üst sınırlarını değiştirmek için See-Saw metodu uygulanır. AND, XOR ve XNOR kapısı sayılarını azaltmayı amaçlar.	Devre derinliği önemsenir ancak doğrusal bileşenlerin yanı sıra, doğrusal olmayan bileşenler de dikkate alınır ve optimize edilir. Sadece doğrusal bileşenlerin optimize edileceği durumlarda yöntemin See-Saw kısmı kullanılmalıdır.
TP19 (sezgisel) [3]	2019	RNBP algoritmasıyla BP10 algoritmasına rastgelelik eklenmiştir. A1 ve A2 optimizasyon algoritmalarında, kuyruk kırma adımında kullanılan öklid normunu ile çözüm sağlanamazsa, rastgelelik adımı sayesinde kuyruk problemi çözülmüş olur.	Devre derinliğini önemsemez.

Literatürde önerilen genel optimizasyon algoritmalarının yanı sıra, yayılım matrislerinin genel devre optimizasyonunu yapan SAT–based [56] ve LIGHTER [57] gibi biçimlendirici (former) araçlar ile Yosys [58] ve ABC [59] gibi hazır devre sentezleyicileri mevcuttur.

Genel optimizasyon yöntemleri, biçimlendirici araçlar ve hazır devre sentezleyicileri sayesinde blok şifrelerin yayılım tabakalarında kullanılan (tersi kendisine eşit) MDS matrislerin donanım üzerinde optimize edilmiş verimli uygulamaları mümkündür.

9.5. SONUÇ VE DEĞERLENDİRMELER

Bu bölümde, blok şifrelerin yayılım tabakaları genel bir bakış açısıyla ele alınmıştır. Bu kapsamda, blok şifrelerdeki yayılma tekniğinin önemi ve yayılmanın hangi bileşenlerle sağlandığı açıklanmıştır. En iyi ve verimli yayılım tabakalarının tasarımı için, (tersi kendisine eşit) MDS matrislerin önemi vurgulanmış, bu matrislerin cebirsel özellikleri detaylarıyla verilmiştir. Bunun yanı sıra (tersi kendisine eşit) MDS matrislerin tasarımı için kullanılan yöntemler, bu yöntemlerin avantajları ve dezavantajları karşılaştırmalı olarak sunulmuştur. Donanım–verimli (tersi kendisine eşit) MDS matrislerin üretilmesi için özellikle XOR sayısı ve devre derinliği parametrelerinin önemi vurgulanmış, bu matrisler için yerel ve genel optimizasyon yöntemleri kıyaslamalı olarak verilmiştir. Genel optimizasyon yöntemlerinde yayılım matrisini oluşturan devrenin tamamı göz önünde bulundurulduğundan, yerel optimizasyon yöntemleri yerine genel optimizasyon yöntemlerinin kullanılması, bir yayılım matrisinin daha düşük XOR sayılı ve minimum devre derinlikli tasarımının gerçeklenmesine olanak sağlar. Genel optimizasyon teknikleri ile bulunması hedeflenen en kısa SLP programı, biçimlendirici araçlar ve hazır devre sentezleyicileri kullanılarak daha da optimize edilir. Bu nedenle farklı yerel optimizasyon yöntemlerinin geliştirilmesinin yanı sıra genel optimizasyon yöntemlerinin de tasarımı önemli birer açık problemdir.

Düşük maliyetli (tersi kendisine eşit) MDS matrislerin üretilmesi için yeni yerel ve genel optimizasyon yöntemlerinin geliştirilmesi açık problem-

leri için olası ileriki çalışmalar ele alındığında, kriptografik açıdan güçlü ve verimli ikili yayılım tabakalarının tasarımı için literatürde yer alan bazı yöntemler [60], [61] yeni ve minimum maliyetli tersi kendisine eşit MDS matrislerin tasarımları için kullanılabilir. Bazı özel matris formlarının kullanımı kaynaklı sonlu cisim üzerinde çalışılan alan, aslında aranılan minimum XOR sayılı ve minimum derinlikli (tersi kendisine eşit) MDS matrisleri içermiyor olabilir. Bu nedenle seçilecek özel boyutlar $(4\times4,\ 8\times8,\ 16\times16)$ için $\mathbb{F}_{2^m}$ sonlu cismi üzerinde özellikle tersi kendisine eşit MDS matrislerin tamamını üretebilen yeni formların tasarlanması önemli çalışmalardır. Genel optimizasyon yöntemleri için; özellikle kuyruk kırma adımı sonunda seçilen aday çiftler arasından seçimler yapılırken adayların farklı istatistiksel dağılımlar göz önünde bulundurularak seçilmesi devreyi oluşturacak derinlik ve XOR sayısının azaltılmasında etkili olacaktır. Bunun yanı sıra yeni SLP programlarının geliştirilmesi olası çözüm önerilerindendir.

Düşük XOR maliyetli ve minimum derinlikli (tersi kendisine eşit) MDS matrislerin üretilmesi literatürde çalışılan önemli açık problemlerden biri olduğu için bu bölüm kapsamında verilen bilgiler diğer çalışmalar için bir rehber niteliği taşıyacaktır.

Teşekkür

Çalışmada, Meltem Kurt Pehlivanoğlu TÜBİTAK 2219-Yurt Dışı Doktora Sonrası Araştırma Burs Programı kapsamında kısmi olarak desteklenmiştir.

KAYNAKLAR

[1] A. Kerckhoffs, La Cryptographie Militaire I-III, Journal des Sciences Militaires, pp. 5–38, 1883.

[2] R. Avanzi, A Salad of Block Ciphers, IACR Cryptology ePrint Archive, Report 2016/1171, 2016.

[3] Q. Q. Tan, T. Peyrin, Improved Heuristics for Short Linear Programs, Cryptology ePrint Archive, Report 2019/847, 2019.

[4] G. Bertoni, J. Daemen, M. Peeters, G. Van Assche, The Making of KECCAK, Cryptologia, Vol. 38, No. 1, pp. 26–60, 2014.

[5] J. Daemen, Cipher ve Hash Function Design Strategies Based On Linear and Differential Cryptanalysis, Katholieke Universiteit Leuven, PhD Thesis, Belgium, 1995.

[6] L.E. Bassham, A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray ve S. Vo, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, Technical Report, United States, 2010.

[7] M.T. Sakallı, Kriptografik Test Yöntemleri Ve Kriptoanaliz, Siber Güvenlik ve Savunma: Problemler ve Çözümler, pp. 87-134, 2019.

[8] S. Sarkar, H. Syed, R. Sadhukhan, D. Mukhopadhyay, Lightweight Design choices for LED-like block ciphers, INDOCRYPT 2017, LNCS, Vol. 10698, pp. 267–281, 2017.

[9] A. Bogdanov vd., PRESENT: An Ultra-Lightweight Block Cipher, CHES 2007, LNCS, Vol. 4727, pp. 450–466, 2007.

[10] L. Knudsen, G. Leander, A. Poschmann, M.J.B. Robshaw, PRINTcipher: A Block Cipher for IC-Printing, CHES 2010, LNCS, Vol. 6225, pp. 16–32, 2010.

[11] P. Barreto, V. Rijmen, The Khazad Legacy Level Block Cipher, First Open NESSIE Workshop, KULeuven, 2000.

[12] P. Barreto, V. Rijmen, The Anubis Block Cipher, available at: http://www.larc.usp.br/pbarreto/anubis-tweak.zip

[13] FX. Standaert, G. Piret, G. Rouvroy, J.-J. Quisquater, JD. Legat, ICEBERG: An Involutional Cipher Efficient for Block Encryption in Reconfigurable Hardware, FSE 2004. LNCS, Vol. 3017, pp. 279–298, 2004.

[14] NIST, Data Encryption Standard, Federal Information Processing Standard (FIPS), Publication 46, U.S. Department of Commerce, Washington D.C., 1977.

[15] J.L. Massey, SAFER K-64: A Byte-oriented Block-ciphering Algorithm, FSE 1993, LNCS, Vol. 809, pp. 1–17,1994.

[16] J.L. Massey, SAFER K-64: One Year Later, FSE 1994, LNCS, Vol. 1008, pp. 212–241, 1995.

[17] D. Wagner, N. Ferguson, B. Schneier, Cryptanalysis of FROG, Proc. 2nd AES Candidate Conference, National Institute of Standards and Technologies, pp. 175–181, 1999.

[18] V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers, E. De Win, The Cipher SHARK, FSE 1996, LNCS, Vol. 1039, pp. 99–111, 1996.

[19] J. Daemen, L. Knudsen, V. Rijmen, The Block Cipher Square, FSE 1997, LNCS, Vol. 1267, pp. 149–165,1997.

[20] J. Daemen, V. Rijmen, The Design of Rijndael: AES - The Advanced Encryption Standard, Information Security and Cryptography, Springer, 2002.

[21] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, Twofish, A Block Encryption Algorithm, In First AES Candidate Conference, National Institute of Standard and Technology, 1998.

[22] K. Aoki vd., Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms — Design and Analysis, SAC 2000, LNCS, Vol. 2012, pp. 39–56, 2001.

[23] K.C. Gupta, I.G. Ray, On Constructions of Involutory MDS Matrices, AFRICACRYPT 2013, LNCS, Vol. 7918, pp. 43-60, 2013.

[24] S. Duval, G. Leurent, MDS Matrices with Lightweight Circuits, IACR Trans. Symmetric Cryptol., Vol. 2018, No. 2, pp. 48–78, 2018.

[25] M. Kurt Pehlivanoğlu, Maksimum Uzaklıkta Ayrılabilen Matrislerin Elde Edilebilmesi İçin Yeni Bir Matris Formu ve Bir Hafif Sıklet Blok Şifreye Uygulaması, Doktora Tezi, Kocaeli Üniversitesi, Kocaeli, Türkiye, 2018.

[26] K.C. Gupta, S.K. Pandey, I.G. Ray, S. Samanta, Cryptographically Significant MDS Matrices Over Finite Fields: A Brief Survey And Some Generalized Results, Advances in Mathematics of Communications, Vol. 13, No. 4, 2019.

[27] K. Khoo, T. Peyrin, A.Y. Poschmann, H. Yap, FOAM: Searching for Hardware-Optimal SPN Structures and Components with a Fair Comparison, CHES 2014, LNCS, Vol. 8731, pp. 433-450, 2014.

[28] R. Zhao, B. Wu, R. Zhang, Q. Zhang, Designing Optimal Implementations of Linear Layers (Full Version), Cryptology ePrint Archive, Report 2016/1118, 2016.

[29] S. Li, S. Sun, C. Li, Z. Wei ve L. Hu, Constructing Low- latency Involutory MDS matrices with Lightweight Circuits, IACR Transactions on Symmetric Cryptology, Vol. 1, pp. 84–117, 2019.

[30] C. Beierle, T. Kranz, G. Leander, Lightweight Multiplication in GF(2^n) with Applications to MDS Matrices, CRYPTO 2016, LNCS, Vol. 9814, pp. 625–653, 2016.

[31] D. Toh, J. Teo, K. Khoo, S.M. Sim, Lightweight MDS Serial-Type Matrices with Minimal Fixed XOR Count, AFRICACRYPT 2018, LNCS, Vol. 10831, pp. 51–71, 2018.

[32] K.C. Gupta, I.G. Ray, On Constructions of MDS Matrices from Companion Matrices for Lightweight Cryptography, CD-ARES 2013, LNCS, Vol. 8128, pp. 29–43, 2013.

[33] T. Kranz, G. Leander, K. Stoffelen, F. Wiemer, Shorter Linear Straight-Line Programs for MDS Matrices, IACR Transactions on Symmetric Cryptology, Vol. 2017, No. 4, pp. 2017.

[34] P.S.L.M. Barreto, M. J. Simplício, CURUPIRA-1, A Block Cipher for Constrained Platforms, 25th Brazilian Symposium on Computer Networks and Distributed Systems, 2007.

[35] T.P. Berger, Construction of Recursive MDS Diffusion Layers from Gabidulin Codes, INDOCRYPT 2013, LNCS, Vol. 8250, pp. 274-285 2013.

[36] D. Augot, M. Finiasz, Direct Construction of Recursive MDS Diffusion Layers Using Shortened BCH Codes, FSE 2014, LNCS, Vol. 8540,pp. 3-17, 2015.

[37] K.C. Gupta, I.G. Ray, Cryptographically Significant MDS Matrices Based on Circulant and Circulant-like Matrices for Lightweight Applications, Cryptogr. Commun., Vol. 7, pp. 257-287, 2015.

[38] P. Junod, S. Vaudenay, Perfect Diffusion Primitives for Block Ciphers, SAC 2004, LNCS, Vol. 3357, pp. 84-99, 2004.

[39] S.M. Sim, K. Khoo, F. Oggier, T. Peyrin, Lightweight MDS Involution Matrices, FSE 2015, LNCS, Vol. 9054, pp. 471-493, 2015.

[40] M. K. Pehlivanoglu, M. T. Sakalli, S. Akleylek, N. Duru ve V. Rijmen, Generalisation of Hadamard Matrix to Generate Involutory MDS Matrices for Lightweight Cryptography, IET Information Security, Vol. 12, pp. 348–355, 2018.

[41] M. Sajadieh, M. Dakhilalian, H. Mala, B. Omoomi, On Construction of Involutory MDS Matrices from Vandermonde Matrices in GF(2^q), Des. Codes Cryptogr., Vol. 64, pp. 287–308, 2012.

[42] J. Guo, T. Peyrin, A. Poschmann, The PHOTON Family of Lightweight Hash Functions, CRYPTO 2011, LNCS, Vol. 6841, pp. 222-239, 2011.

[43] S. Wu, M. Wang, W. Wu, Recursive Diffusion Layers for (Lightweight) Block Ciphers and Hash Functions, SAC 2012, LNCS, Vol. 7707, pp. 355–371, 2013.

[44] H. Xu, Y. Zheng, X. Lai, Construction of Perfect Diffusion Layers from Linear Feedback Shift Registers, IET Information Security, Vol. 9, No. 2, pp. 127–135, 2015.

[45] K.C. Gupta, S.K. Pandey, A. Venkateswarlu, On the Direct Construction of Recursive MDS Matrices, Designs, Codes and Cryptography, Vol. 82, pp. 77-94, 2017.

[46] S. Sarkar, H. Syed, Analysis of Toeplitz MDS Matrices, ACISP 2017, LNCS, Vol. 10343, pp. 3-18, 2017.

[47] Q. Li, B. Wu, Z. Liu, Direct Constructions of (Involutory) MDS Matrices from Block Vandermonde and Cauchy-Like Matrices, WAIFI 2018, LNCS, Vol. 11321, pp. 275–290, 2018.

[48] A. Visconti, C. V. Schiavo, R. Peralta, Improved upperbounds for the expected circuit complexity of dense systems of linear equations over GF(2), Inf. Process. Lett., Vol. 137, pp. 1–5, 2018.

[49] C. Paar, Optimized Arithmetic for Reed-Solomon Encoders, 1997 IEEE International Symposium on Information Theory, pp. 250, 1997.

[50] J. Boyar, R. Peralta, A New Combinational Logic Minimization Technique with Applications to Cryptology, SEA 2010, LNCS, Vol. 6049, pp. 178-189, 2010.

[51] J. Boyar, P. Matthews, R. Peralta, Logic Minimization Techniques with Applications to Cryptology, Journal of Cryptology, Vol. 26, pp. 280–312, 2013.

[52] J. Boyar, M. G. Find, R. Peralta, Low-Depth, Low-Size Circuits for Cryptographic Applications, BFA 2017. 2017.

[53] J. Boyar, M. G. Find, R. Peralta, Small Low-depth Circuits for Cryptographic Applications, Cryptography and Communications, Vol. 11, No. 1, pp. 109–127, 2019.

[54] G.G. Guzel, M.T. Sakallı, S. Akleylek, V. Rijmen, Y. Çengellenmiş, A New Matrix Form to Generate All 3 × 3 Involutory MDS Matrices over $\mathbb{F}_{2^m}$, Information Processing Letters, Vol.147, pp. 61-68, 2019

[55] M.T. Sakallı, S. Akleylek, K.Akkanat, V. Rijmen, On the Automorphisms and Isomorphisms of MDS Matrices and their Efficient Implementations, Turkish Journal of Electrical Engineering and Computer Science, Vol. 28, No. 1, pp. 275-289, 2020.

[56] K. Stoffelen, Optimizing S-Box Implementations for Several Criteria Using SAT Solvers, FSE 2016, LNCS, Vol. 9783 pp. 140–160. Springer, 2016.

[57] J. Jean, T. Peyrin, S.M. Sim, J. Tourteaux, Optimizing Implementations of Lightweight Building Blocks, IACR Trans. Symmetric Cryptol., Vol. 2017, No. 4, pp. 130–168, 2017.

[58] C. Wolf, Yosys Open Synthesis Suite, available at: http://www.clifford.at/yosys/.

[59] R.K. Brayton, A. Mishchenko, {ABC:} An Academic Industrial Strength Verification Tool, CAV 2010, Vol. 6174, LNCS, pp. 24–40, 2010.

[60] S. Akleylek, V. Rijmen, M.T. Sakallı, E. Öztürk, Efficient Methods to Generate Cryptographically Significant Binary Diffusion Layers, IET Information Security, Vol. 11, No. 4, pp. 177-187,2017.

[61] M.T. Sakallı, S. Akleylek, B. Aslan, E. Buluş, F. Büyüksaraçoğlu Sakallı, On the Construction of 20 × 20 and 24 × 24 Binary Matrices with Good Implementation Properties for Lightweight Block Ciphers and Hash Functions, Mathematical Problems in Engineering, Vol. 2014, pp. 1-13, 2014.

Bölüm 10

GÜVENLİK UYGULAMALARINI HEDEFLEYEN FİZİKSEL SALDIRILAR VE BUNLARA KARŞI ALINABİLECEK ÖNLEMLER

Meltem Kurt Pehlivanoğlu - Elif Bilge Kavun

Bu bölümde özellikle güvenlik uygulamalarında kullanılan donanım ve yazılım bileşenlerini hedef alan, bu bileşenler kaynaklı sistem güvenlik açıklarını ve tehditlerini anlamayı amaçlayan, bozucu (invasive), bozucu olmayan (non - invasive) ve yarı bozucu (semi - invasive) fiziksel saldırı türlerinin kapsamlı incelemesine yer verilmektedir. Fiziksel saldırıdan kasıt, yetkilendirme (authorization) olmadan, kriptografik bileşenlerin veya kriptografik algoritmaların özellikle yazılım ve donanım uygulamalarının zayıflığından faydalanılarak sistem hakkında anlamlı bilgi çıkarımıdır. Bu bölümde ayrıca, fiziksel saldırılara karşı alınabilecek mevcut önlemler ve bu önlemlerin güvenlik incelemeleri üzerine temel bir altyapı sunulmaktadır. Bunun yanı sıra, kriptografik bileşenlerin ve güvenlik protokollerinin donanım ve yazılım uygulamaları için güvenlik değerlendirmeleri detaylandırılmıştır.

10.1. GİRİŞ

Güvenlik uygulamalarının tasarım temelinde, kriptografi ve kriptanaliz yöntemlerini içeren kriptoloji bilimi yatar. Kriptografi, güvensiz haberleşme ortamı üzerinden, gönderici ve alıcı tarafları arasında verinin gizlilik (confidentiality), bütünlük (integrity) ve kullanılabilirlik (availability) gibi bilgi güvenliği ilkelerine bağlı kalarak iletilmesini sağlayan yöntemlerdir (diğer bir ifadeyle bir kriptosistemin bütünüdür). Kriptanaliz ise, kriptosistemlerin teorik zayıf-

lıklarından faydalanılarak, matematiksel analizinin yapılması (kriptosistemin kırılması) anlamına gelir. Kriptanaliz saldırılarına dayanıklı bir kriptosistem tasarımı önemli açık problemlerden biridir. Kriptografi ve kriptanaliz alt dallarından oluşan kriptoloji bilimi, verinin bütünüyle korunması ve alıcı tarafına iletilmesi amaçlı, kriptografik algoritmaların (örneğin şifreleme algoritmaları) veya kriptografik yapıların tasarımı ve bu sistemlerin güvenlik seviyelerinin arttırılması ile ilgilenir. Şifreleme algoritmaları tasarımında kullanılan önemli bileşenler, bu bileşenlerin güvenlik uygulamaları ve kriptanaliz yöntemleriyle ilgili kapsamlı bilgiye [1], [2]'den erişilebilir.

Teknolojinin gelişmesiyle artan kaynak kısıtlı cihaz kullanımı güvenlik risklerini de beraberinde getirir. Azaltılmış güç tüketimi, daha az hesaplama gücü, daha az bellek kullanımı ve daha az güç kaynağı gereksinimine sahip bu cihazlar, özellikle donanım güvenlik açıklarından faydalanan fiziksel saldırılara da maruz kalırlar. Düşük işlem gücü ve düşük bellek kapasitesiyle bu cihazlar için yüksek seviyeli güvenlik çözümlerinin sağlanması açık problemlerden biridir. Fiziksel saldırılar, donanımsal cihaza (örneğin çipe) doğrudan erişim veya en azından ölçüm yapabilecek yakınlıkta olmayı gerektiren, cihazlardan bilgi sızdırmayı veya cihaz işleyişini manipüle etmeyi amaçlayan saldırılardır. Ağ katmanı ya da yazılım katmanı saldırılarının aksine özel donanım, araç ve bilgi birikimi sahibi olmayı da gerektirirler. Kullanım alanı genellikle şifreleme veya kimlik doğrulama adımlarının (authentication) atlanmasına dayanır. Bu durumda bilgi sızdırmayı sağlayan bileşen şifreleme algoritmasının gizli anahtarı olur. Fiziksel saldırıların kriptoanalizden temel farkı, şifreleme algoritmasının güvenlik açığından değil bu algoritmanın gerçeklenmesindeki hatalardan yararlanmasıdır. Diğer bir ifadeyle, kriptoanalizde algoritma matematiksel olarak analiz edilerek algoritmanın açıkları tespit edilirken, fiziksel saldırılarda algoritmanın gerçeklenmesindeki ve çalıştırılan cihaz üzerindeki güvenlik açıklarına odaklanılır.

Bu bölümde kriptosistemler için önemli bir tehdit oluşturan fiziksel saldırı türleri, bu saldırılara sebep olan güvenlik açıkları ve bu güvenlik açıklarına karşı alınacak önlemler kapsamlı bir şekilde sunulmuştur.

Çalışmanın ilerleyen bölümleri şu şekilde düzenlenmiştir; Bölüm 10.2'de fiziksel saldırılar sınıflandırılarak, her bir sınıfa ait saldırılar açıklanmış ve bu saldırının hedef aldığı güvenlik açıkları verilmiştir. Bölüm 10.3'te ise sı-

nıflandırılan her bir fiziksel saldırıya karşı alınabilecek önlemler verilerek, sonrasında bu önlemler gruplandırılarak özetlenmiştir. Son bölümde ise çalışmada verilen kapsamlı bilgiler özetlenmiştir.

10.2. FİZİKSEL SALDIRILAR

Bu bölümde fiziksel saldırıların sınıflandırılması ve fiziksel saldırı türleri ele alınmaktadır. Fiziksel saldırılar uygulandığı devre üzerinde yarattığı etki açısından bozucu saldırılar, bozucu olmayan saldırılar ve yarı bozucu saldırılar olmak üzere üç ana grupta sınıflandırılmaktadır. Tablo 10.1'de fiziksel saldırı sınıfları ve bu sınıflarda yer alan saldırı türleri verilmiştir.

Tablo 10.1. Fiziksel Saldırıların Sınıflandırılması

Bozucu Saldırılar	Bozucu Olmayan Saldırılar	Yarı Bozucu Saldırılar
Tersine Mühendislik (Reverse Engineering)	Yan Kanal Saldırıları (Side Channel Attacks)	Ultraviyole (Morötesi) Işın Saldırıları (Ultraviolet – UV Attacks)
Derinlemesine Araştırma (Microprobing)	Kaba Kuvvet Saldırıları (Brute Force Attacks)	İleri Görüntüleme Saldırıları (Advanced Imaging Attacks)
-	Hata Oluşturma Saldırıları (Fault Injection Attacks)	Aktif Foton Problama (Active Photon Probing)
-	Veri Kalıntısı Saldırıları (Data Remanence)	Optik Hata Oluşturma Saldırıları (Optical Fault Injection Attacks)

Her sınıfa ait fiziksel saldırı türleri aşağıdaki alt bölümlerde verilmiştir.

10.2.1. Bozucu Saldırılar

Bozucu saldırılar isminden de anlaşılacağı üzere uygulandığı devreyi kullanılmaz hâle getirir ya da saldırı gerçekleştiğine dair delil bırakır. Bozucu saldırılar, kullanılan çipin iç bileşenlerine doğrudan erişebilmek için cihazın açılması (depackaging) işlemini gerektirir. Bu işlem sırasıyla;

- paketten çıkarma (decapsulation) ve
- çıkarılan katmanların ayrı ayrı işlenmesi (deprocessing)

aşamalarından oluşur. Şekil 10.1'de bu adımlarda yapılan işler verilmiştir.

Şekil 10.1. Bozucu Saldırıların İşlem Aşamaları

Paketten çıkarma işlemi sonunda cihazın çipi açığa çıkar. Bu işlem nitrik asit kullanılarak elle yapılabileceği gibi paketten çıkarma makineleri ile de çok daha masraflı ancak uğraşsız şekilde uygulanabilir. Paketten çıkarma aşamasından sonra, birden fazla katmana sahip karmaşık çiplerin incelenebilmesi için katmanlarının teker teker çıkarılması/birbirinden ayrılması ve işlenmesi gerekir.

Çip hakkında bilgi edinmek için tersine mühendislik ve/veya derinlemesine araştırma işlemi yapılır. Tersine mühendislik, dijital kameralı optik mikroskop kullanılarak çipin katman katman incelenmesi, transistör ve ara bağlantıların haritalanması ve bu bilgiler üzerine çalışılmasıdır. Tersine mühendislik, bellek tiplerinden bilgi okunarak, cihazın iç yapısını ve işlevini öğrenmeyi amaçlar. Saldırgan, veri ve adres yolu bağlantı yapılarını inceleyerek ROM (Read-only memory – Salt Okunabilir Bellek), SRAM (Static random-access memory – Statik Rastgele Erişimli Bellek), EEPROM (Electrically erasable programmable read-only memory – Elektriksel Olarak Silinebilir Salt Okunur Bellek) ve ALU (Arithmetic Logic Unit – Aritmetik Mantık Birimi) gibi birimleri tanımlayabilir [3].

Derinlemesine araştırma ile devre/çipin optik mikroskop altında detaylı ve hassas olarak incelenmesiyle, devrenin iç yüzeyine doğrudan müdahale edilmesi sağlanır. Bu işlem için öncelikle lazer kesici ile pasivasyon olarak adlandırılan devreyi örten ve alüminyum bağlantı hatları ve iyon saldırısından

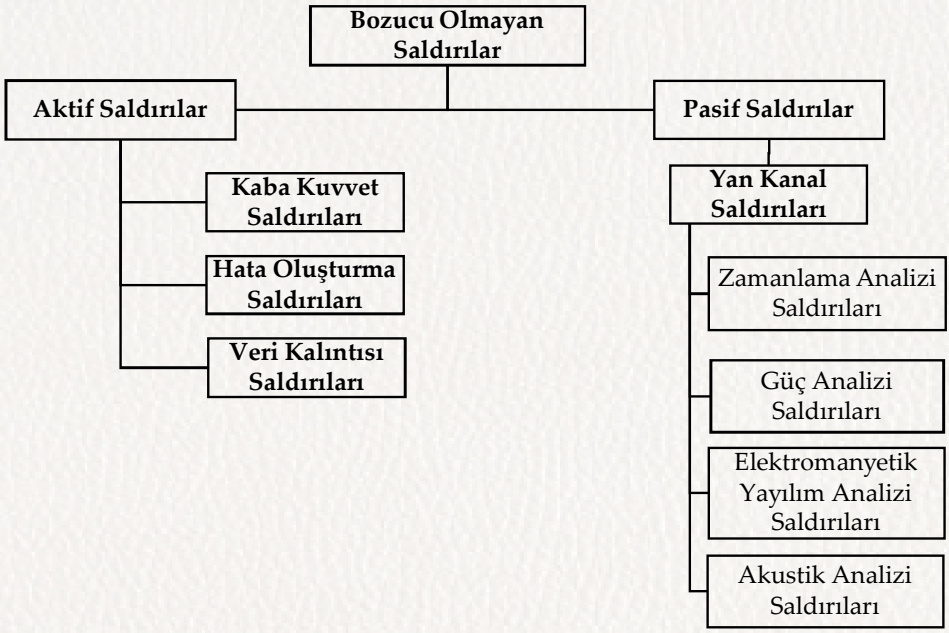
koruyan tabaka kaldırılmalı veya delinmelidir. Daha sonra derinlemesine araştırma istasyonu kullanılarak derinlemesine araştırma işlemi başlatılır ve çip hakkında detaylı bilgi edinilir. Bu aşamada çip üzerindeki aktiviteler izlenebilir, bellekten gizli anahtar gibi bilgiler edinilebilir ve hatta test sinyalleri gönderilip sonuçlar okunabilir. Son olarak çip üzerinde değişiklik yapılır veya cihazın kopyası istenilen değişiklikler ile üretilir. Cihaz hakkında elde edilen bilgilerden sonra yapılacak değişiklik tespit edilir. Bu değişiklik bir veri yolunun kesilmesi olabilir. Değişikliklerin uygulanabilmesi için FIB (Focused Ion Beam–Odaklanmış İyon Demeti) istasyonları kullanılabilir. FIB uygulamak için (çoğunlukla tersine mühendislik ile) cihazla ilgili detaylı bilgi sahibi olmak gereklidir.

Bozucu saldırıların tipik bir örneği, veri transferlerini görmek için veri yoluna bir kablonun bağlanmasıdır [4]. Bozucu saldırılar ile ilgili kapsamlı bilgiye [5]'ten erişilebilir.

10.2.2. Bozucu Olmayan Saldırılar

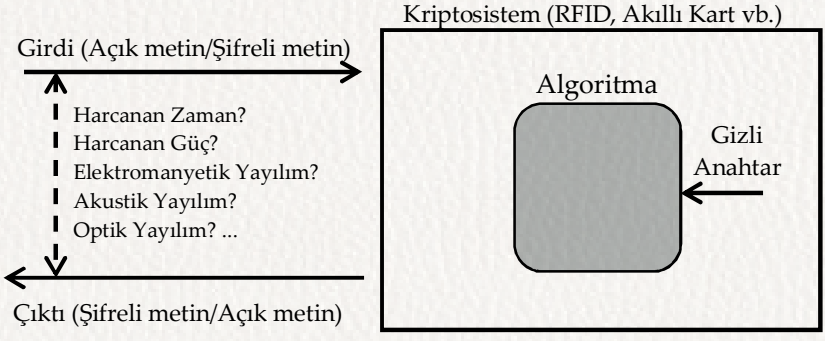
Bozucu olmayan saldırıların uygulanması için paketten çıkarma, katmanlarına ayırma gibi herhangi bir ön hazırlık gerektirmez. Bu saldırılar sırasında cihaza zarar verilmez ve saldırı gerçekleştiğine dair herhangi bir iz bırakılmaz. Cihaz veya çip ile doğrudan değil voltaj, akım, iç saat (clock), giriş/çıkış (Input/Output – I/O) gibi arayüzler üzerinden temasa geçilir. Bu gibi temaslar cihaza bağlanacak bir test çipi ile basitçe gerçekleştirilebilir. Bozucu olmayan saldırılar genel olarak masraflı değildir.

Bozucu olmayan saldırılar davranış açısından pasif ve aktif olarak ikiye ayrılır. Pasif saldırılar uygulanırken fiziksel özellikler yalnızca gözlemlenir veya ölçülür. Aktif saldırılar uygulanırken ise, sistemde işlev bozukluğu yaratmak için aynı zamanda sisteme müdahale edilir [4]. Bozucu olmayan saldırılar yan kanal saldırıları, kaba kuvvet saldırıları, hata oluşturma saldırıları ve veri kalıntısı saldırıları olarak sınıflandırılabilir. Yan kanal saldırıları pasif saldırılar olup, kaba kuvvet saldırıları, hata oluşturma saldırıları ve veri kalıntısı saldırıları aktif saldırılardır. Yan kanal saldırıları temel olarak, farklı ölçüm metriklerine göre zamanlama analizi, güç analizi, elektromanyetik yayılım analizi, akustik analizi saldırıları olarak sınıflandırılabilirler. Şekil 10.2'de bozucu olmayan saldırıların sınıflandırılması gösterilmektedir. Bunun yanı sıra yan kanal saldırıları aktif saldırılarla birlikte kullanılabilir.



Şekil 10.2. Bozucu Olmayan Saldırıların Sınıflandırılması

Yan kanal saldırıları, genel olarak kriptosistem üzerinde çeşitli izlemeler ve ölçümler yaparak ve bu ölçümleri işleyerek bilgi sızdırmak olarak tanımlanabilir. Şekil 10.3'te de verildiği gibi bu ölçümler çalışma zamanı [6], güç tüketimi [7], elektromanyetik radyasyon [8], optik [9], akustik [10], çıktı sinyalleri [11] yan kanal bilgileri (sızıntıları) olabilir.



Şekil 10.3. Kriptosistemlerde Ortaya Çıkabilecek Yan Kanal Bilgileri

Yan kanal saldırıları, bozucu olmayan ve pasif saldırılar olduğundan; bozucu saldırılar ile bozucu olmayan ve aktif saldırılara kıyasla ucuz donanım kullanılarak gerçekleştirilir. Bu nedenle, çoğu kriptografik cihaz (kişisel bilgisayarlardan, akıllı kartlar ve RFID (Radio-Frequency Identification–Radyo Frekanslı Tanıma) gibi küçük gömülü cihazlara kadar) için ciddi bir tehdit oluştururlar [4]. Yan kanal saldırıları ile elde edilen ölçümler sayesinde, kriptosistem üzerinde açık metin ile şifreli metin arasındaki ilişki bilinmeden gizli anahtar ortaya çıkarılabilir. Gizli anahtar bir kez elde edildiğinde şifreli metnin çözülmesi önemli değildir. Gizli anahtarı bulmanın temel yaklaşımı, kriptosistemin gerçek makinelerdeki uygulamasından faydalanılarak, şifreleme ve şifre çözme işlemleri sırasında farklı yan kanal sızıntıları ölçümleri ile elde edilen değerlerin işlenmesidir [12]. Diğer bir yandan, CPU (Central Processing Unit–Merkezî İşlemci Birimi) ve RAM (Random Access Memory–Rastgele Erişimli Bellek) arasındaki performans boşluğunu kapatan ön bellekler (cache) üzerine de saldırılar yapılmaktadır. Ön bellekte oluşan yakalama (hit) ve kaçırma (miss) işlemleri arasındaki zaman farkı yan kanal saldırıları için güvenlik açıkları oluşturmaktadır [13]. Son yıllarda bu saldırılar, makine öğrenmesi, derin öğrenme yöntemleri kullanılarak gerçekleştirilmektedir [14], [15].

Yan kanal saldırıları; kullanılan yan kanal bilgisine göre aşağıdaki gibi sınıflandırılabilir;

- Zamanlama Analizi,
- Güç Analizi,
- Elektromanyetik Yayılım Analizi,
- Akustik Analizi.

Bir kriptosistemde ortaya çıkabilecek sızıntı kanalları temelde depolama (storage) ve zamanlama (timing) kanalları olarak sınıflandırılabilir [16]. Depolama kanallarının aksine zamanlama kanallarından zamanlama değişimi ile faydalanabilir. Depolama kanalları, yazılımda doğrudan görülebilecek yazmaç (register) değeri, sistem çağrısı geri dönüş değeri gibi sistemin bazı fonksiyonel yönlerini ortaya çıkarırken, zamanlama kanalları ise sistemin tamamen işlevsel davranışını ortaya çıkarabilen kanallardır [17].

Zamanlama analizi saldırılarında amaç, kriptosistemin bir işlemi çalıştırırken harcadığı zaman üzerinden hassas bilgileri (örneğin gizli anahtar) elde etmektir. Bir kriptosistemdeki performans karakteristikleri gizli anahtar ve

girdi (açık metin/şifreli metin) ikilisine bağlıdır. Kocher 1996 yılında yaptığı çalışmasında [6], zamanlama kanallarından yapılacak ölçümlerin zamanlama analizi saldırısında kullanılabileceği fikrini ilk kez ortaya atmıştır. Bu fikir, bir kriptosistemde farklı girdi verilerinin işlenmesi (şifreleme/şifre çözme) için geçen sürelerin de, şifreleme algoritmasında yer alan dallanma, koşul durumları, RAM – ön bellek veri aktarımı arasındaki zaman farkı, kullanılan komut kümeleri (IS–Instruction Set) işlemlerinden (çarpma, bölme vb.) dolayı birbirlerinden farklı olacağı düşüncesine dayanır. Çalışmada, özellikle RSA (Rivest–Shamir–Adleman) ve Diffie–Hellman algoritmaları için zamanlama analizi saldırısı yapılmasını önleyen yöntemler verilmiştir. Dhem ve arkadaşları 1998 yılındaki çalışmalarında [18], ilk defa Kocher tarafından ortaya atılan bu fikrin pratik bir uygulamasını gerçekleştirerek, zamanlama analizi saldırısı ile CASCADE akıllı kartı üzerinde gizli anahtarları elde etmişlerdir.

Algoritma 3.1'de, gerçek şifre (*şifre*) ile kullanıcının girdiği şifre bilgisinin (*giriş*) aynı olup olmadığı kontrolünü yapan *karsilastir* fonksiyonunun sözde kodu verilmiştir. Bu fonksiyonun şifreleme algoritması uygulandıktan sonra kullanıldığı varsayıldığında güvenlik açığı oluşturması beklenir. Bu kod parçası gerçek şifre ve girilen şifreyi başarılı bir şekilde karşılaştırır, yazılımsal bir hata içermez. Ancak yan kanal saldırılarına karşı güvensiz bir koddur. Kodun çalışma zamanı, girişin şifreye yakınlığı ile doğrusal olarak artmaktadır. Bu kod üzerinde rakamlardan $\{0,1,\ldots 9\}$ oluşan 4 haneli bir şifrenin kırılması için en kötü koşulda kaba kuvvet ile $10,000 = (10 \times 10 \times 10 \times 10)$ deneme yapmak gerekirken zamanlama analizi saldırısı ile $40 = (4 \times 10)$ deneme yeterli olacaktır. Şifreye harf ve sembollerin de dâhil olması ve şifre uzunluğunun artmasıyla kaba kuvvet ve zamanlama analizi saldırılarının deneme sayıları arasındaki fark daha da yükselecektir. Çünkü kaba kuvvet $O(n^m)$, zamanlama analizi saldırısı ise $O(n \times m)$ zaman karmaşıklığı ile çalışır. Benzer şekilde kod içerisinde özellikle kullanıcı yetkilendirmesi kontrolleri, şifre çözme sırasında tamamlama (padding) hatalarının kontrolleri sırasında meydana gelen zaman farkları zamanlama analizi için yan kanal sızıntıları oluşturur [19].

Algoritma 10.1: Örnek Sözde Kod Parçası

```
1. func karsilastir (sifre, giris) {
2. if uzunluk(sifre) ≠ uzunluk(giris)
3. return false
4. for i = 0 to uzunluk(sifre)
```

5. if sifre[i] ≠ giriş[i]
6. return false
7. end for
8. return true }

Son yıllarda yapılan çalışmalar incelendiğinde mikro-mimariler (microarchitecture) üzerine zamanlama analizi saldırılarına yönelik çalışmaların da arttığı açıktır. Mikro-mimari temelde verilen bir ISA mimarisinin (Instruction Set Architecture–Komut Kümesi Mimarisi) donanıma nasıl uygulanacağını belirler. Ancak mikro-mimariler işlevsel olarak transparan olsalar da, program çalışma zamanı boyunca gözlemlenebilecek bazı gizli durumları içerirler. Mikro-mimariler ön bellek, ALU, kontrol birimleri, veri yolu, dallanma belirleyiciler (branch predictors) gibi önemli bileşenlere sahiptir. Bu nedenle zamanlama değişimleri göz önünde bulundurularak; mikro-mimari bileşenleri üzerinde kargaşa yaratılması, değişim sonuçlarının bulunması, hangi bileşenlerin gizli veriye bağlı olduğunun bulunması amaçlı saldırılar yapılmaktadır [20]. Bunun yanında yazılım tabanlı mikro-mimari saldırıları da, (kısmen) mikro-mimari optimizasyonlarından kaynaklanan zamanlama ve davranış farklılıklarından yararlanır. Genel olarak yazılım tabanlı mikro-mimari saldırıları fiziksel erişim gerektirmez, bunun yerine hedef sistem üzerinde sadece bir tür kod yürütülmesi gerektirir. Ön bellek zamanlama saldırıları, yazılım tabanlı mikro mimari saldırılarının en önemli sınıfıdır [21]. Ön bellek zamanlama saldırıları ilk olarak yazılım tabanlı saldırılarda kriptografik algoritmalara uygulanmıştır [22], [23].

Güç analizi saldırıları, cihazların güç tüketimi özelliklerine odaklanarak, kriptosistemdeki gizli anahtar hakkında bilgi sızdırmayı sağlar. Maliyeti düşük saldırılardır ve temelde kriptosistemin anlık güç tüketiminin; şifrelenen/şifresi çözülen veriye (veri bağımlılığı) ve algoritmada yapılan işlemlere (işlem bağımlılığı) bağlı olmasından yararlanır. Veri bağımlılığından kasıt, devre içindeki lojik kapıların güç tüketiminin giriş değerine (veriye) bağlı dinamik olarak değişmesidir. İşlem bağımlılığından kasıt ise, her işlemin farklı güç tüketim karakteristiğine sahip olmasıdır. Bu saldırılarda en basit düzenek, kriptografik cihaz ile kaynak arasına, gerilim farklarını tespit etmek amaçlı bir direnç yerleştirilmesidir [24]. Güç analizi saldırısı ilk kez Kocher ve arkadaşlarının, 1999 yılındaki çalışmasında [7] yapılmıştır. Güç analizi saldırıları; Basit Güç Analizi (Simple Power Analysis) [7], Farksal Güç Analizi (Diffe-

rential Power Analysis) [7] ve Korelasyon Güç Analizi (Correlation Power Analysis) [25] olarak sınıflandırılır. Basit güç analizinde, herhangi bir istatistiksel yöntem kullanılmadan, tek bir güç tüketiminin ölçümü yapılır, daha sonra işlemler ile güç tüketim izleri arasındaki bağıntı gözlemlenerek yorumlanır. Farksal güç analizi ve korelasyon güç analizinde ise, aynı gizli anahtar kullanılarak kriptosistemde yer alan algoritmadan çoklu güç izleri toplanır ve bu izler üzerinde istatistiksel analizler yapılır. Farksal güç analizi, güç tüketimi ile belirli anahtara bağlı bitler arasındaki korelasyonu kullanır. Saldırgan gizli anahtarın bir biti için bir tahmin yapar, sonrasında bu güç izlerini tahmine bağlı olarak üretilen yazmaç değerine (register value) göre bölümler ve sonrasında bu bölümlerin anlamlı fark gösterip göstermediğini kontrol eder. Korelasyon güç analizi saldırıları ise, farksal güç analizi saldırılarından farklı olarak, güç izleri ve yazmaç değeri arasındaki korelasyon katsayısının hesaplanmasına dayanır.

Elektromanyetik yayılım analizinde, devredeki lojik kapıların girdi verisine göre farklı akım çekmesine bağlı olarak devreden yayılan elektromanyetik bilgiler kullanılır. Kocher ve arkadaşları çalışmalarında [7], elektromanyetik yayılımların da güç tüketimlerine ek olarak saldırı için kullanılabileceğine değinmişlerdir. Bu analizle pasif olarak hem işlenen dâhilî işlemler (internal operations), hem de işlemin verisi elde edilebilir. Küçük manyetik döngü antenler kullanılarak kriptografik cihazlar üzerinden elektromanyetik yayılımların tespit edilebileceği gösterilmiştir [26]. Elektromanyetik sinyaller bir döngü anteni tarafından yakalandığında, verilerin analizde kullanılabilmesi için dijital örnekleme gerekir. Teorik olarak, elektromanyetik sinyal örnekleme ekipmanının örnekleme hızı, yakalanması gereken maksimum elektromanyetik frekansının iki katı olmalıdır, bu nedenle bu cihazlar çok yüksek örnekleme hızına sahip olmalıdır [27]. Yüksek örnekleme hızına sahip osiloskoplar ve spektrum analiz cihazları en yaygın kullanılan örnekleme cihazlarıdır. Bu cihazların yakaladığı sayısallaştırılmış veriler daha sonra sinyal analiz yazılımında analiz edilebilir. SDR (Software Defined Radios – Yazılım Tabanlı Radyolar) ayrıca elektromanyetik sinyalleri analiz için kullanılır. Bunun yanında işlemciler de elektromanyetik yayılımlara sebep olurlar, bu yayılımları tespit etmenin en kolay yöntemi şüpheli elektromanyetik sinyalleri geniş frekans spektrumunda taramaktır, daha sonra bu tanımlanmış sinyaller yan kanal bilgisi olarak kullanılır [28], [29]. Şöyle ki; işlemci yazmacındaki bir bit ‘0’ değerinden ‘1’ değerine değiştiğinde çok yüksek enerji tüketimine neden olur.

Buradan işlemci yazmacındaki tüm içeriklerin, bir önceki durumu ile yeni durumu arasındaki Hamming mesafesi elektromanyetik yayılım yan kanal bilgisi olarak kullanılır. Aynı zamanda hedef cihazın sistem saati elektromanyetik yayılımın ana kaynağıdır [27]. Elektromanyetik yayılım analizi, Basit Elektromanyetik Yayılım Analizi (Simple Electromagnetic Analysis) ve Farksal Elektromanyetik Yayılım Analizi (Differential Electromagnetic Analysis) olarak sınıflandırılır. Basit elektromanyetik yayılım analizi, basit güç analizi ile benzer şekilde gözlemlemeye dayanır. Temelde, elektromanyetik izler frekans düzlemine dönüştürülür ve bir spektrogram olarak çizilir bu da birden fazla frekans üzerinde farklı sinyal modellerinin (patterns) gözlemlenmesini sağlar. Farksal elektromanyetik yayılım analiz ise, farksal güç analizine benzer şekilde, gözlemleyerek bilgi çıkarımının yetmediği çok sayıda elektromanyetik yayılım izlerinin bulunduğu durumlarda kullanılır [30].

Akustik analiz saldırılarında kriptosistemden çıkan sesler incelenir. Fan gürültüsü, kondansatör ve indüktörlerin çalışırken çıkardıkları ultrasonik sesler, klavye üzerindeki tuş vuruşları gibi sesler saldırı için yan kanal bilgisi olarak kullanılabilir. Akustik analiz saldırılarıyla ilgili çalışmalar incelendiğinde; nokta vuruşlu yazıcıların baskı sesinin analiz edilmesiyle baskı içeriğinin elde edilmesi [31], üç boyutlu yazıcı ile basılan nesnenin yayılan sesle yeniden oluşturması [32], Enigma makinesi üzerinde basılan tuşlardan yayılan sesler sayesinde anahtarın elde edilmesi [33], fiziksel klavye üzerinden girilen anahtar bilgilerinin sınıflandırılması, jiroskop ve mikrofon kullanılarak cep telefonunda sanal klavye üzerindeki tuş vuruşlarının tahmin edilmesi [34] gibi birçok çalışmanın olduğu görülebilir. Akustik analiz saldırıları pasif yan kanal saldırılardır ancak Cheng ve arkadaşlarının 2019 yılındaki çalışmasında [35] ilk aktif akustik yan kanal saldırısı verilmiştir.

Kaba kuvvet saldırıları, en basit ve en güçlü saldırılardan biridir ve bu saldırı türü anahtar uzayındaki tüm anahtarları hesaplayarak anlamlı açık metni döndüren tek bir anahtarı arar. Eğer saldırgan yeterli zaman ve hesaplama gücüne sahipse birçok kriptosistem bu saldırısı ile kırılabilir, OTP (One-Time Pad - Tek Kullanımlık Şerit) bu saldırılara karşı bilinen en güvenli kriptosistemdir. Ayrıca bu saldırı ile yüksek veya düşük voltaj değerleri ya da rastgele sinyaller üretilerek cihazın fabrika moduna erişimi sağlanabilir [36].

Hata oluşturma saldırıları, sisteme beklenmedik ya da hatalı girişler verip çıktıyı gözlemleyerek gizli anahtarları ortaya çıkarma ya da saldırgana yet-

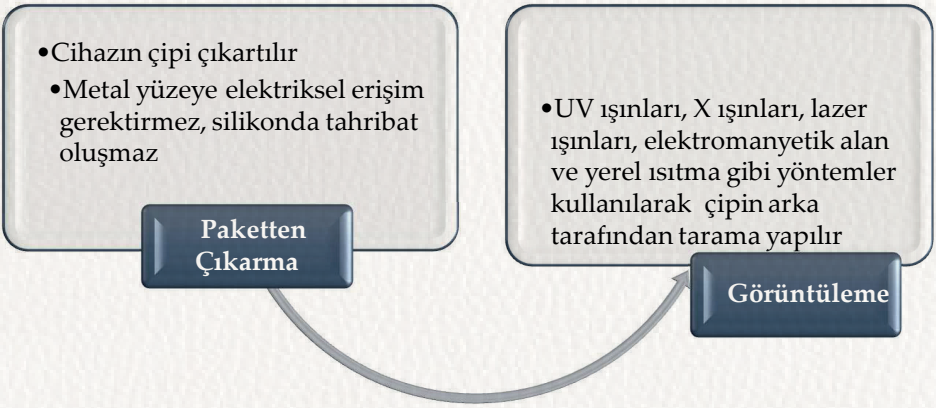
kilendirme sağlayan saldırılardır. Kriptosistemdeki hata süresi geçici veya harmonik, hata etkisi veriyi değiştirme veya akışı değiştirme, hata hedefi ise güvenlik kontrolünü geçme, bozulma hesaplama veya sapma (bias) girdileri olarak gruplandırılabilir. Bunun yanında enjekte edilebilecek hata modelleri; tek bir biti veya birden fazla biti değiştirme (hedef bir veya birden fazla bit değiştirilir), rastgele byte hatası oluşturma (byte içinde yer alan bitlerin rastgele değiştirilmesi), komut atlama (yazılım içinde yer alan kodun bir veya birkaç satırının işlenmeden geçirilmesi), takılma hatası oluşturma (hedefte 0/1 değerleri arasında takılma meydana getirme) olarak sınıflandırılabilir. Çoğu zaman güvenli sistemlerde hatalı girişler ön kontrolden geçer ve kabul edilmez. Bu yüzden hatalı verinin sisteme enjekte edilmesi gerekir. Hata enjekte yöntemleri düşük maliyetli ve genel (low cost and global), yüksek maliyetli ve yerel (high cost and local) olarak ayrılabilir. Düşük maliyetli ve genel yöntemler, çok sayıda cihaza uygulanabilir olup, saldırının uygulanması için az uzmanlık gerektirirler, bu saldırılar güç hataları (power glitch), sistem saati kurcalama (clock tampering) ve sıcaklık değişimi (temperature variation) olarak sınıflandırılır. Yüksek maliyetli ve yerel yöntemler ise yüksek uzmanlık ve pahalı donanımlar gerektiren saldırılardır, bu saldırılar ışık/lazer ışını enjeksiyonu (light/laser injection), elektromanyetik akı enjeksiyonu (electromagnetic injection), FIB enjeksiyonu olarak sınıflandırılabilir. Şöyle ki, çipin beyaz ışık ve lazere karşı hassasiyeti kullanılarak transistör ve flip-flopların durumu değiştirilebilir. Bu işlem X ışınları (X-ray), iyon demeti veya elektromanyetik akı kullanılarak da uygulanabilir [37].

Veri kalıntısı problemi ilk olarak manyetik ortamlarda fark edilmiştir [38]. Silme veya üzerine yazma (overwrite) işleminden sonra bellekte kalan veriyi geri getirmek Veri kalıntısı saldırıları ile mümkündür. Bu durumda, gizli anahtarlar bellekten silindiği hâlde veri kalıntıları ile çıkarılabilirse, önceden şifrelenmiş bilgilerin gizliliği etkilenebilir. SRAM belleklerde, düşük sıcaklıklarda veriler dakikalar seviyesinde dondurulup o verilere erişilebilir. Yapılan çalışmada [38], verilerin -20°C altında donduğu, sıcaklık daha da düşürüldüğünde veri kalıntısı olarak kullanılabilecek verilerin sayısının arttığı gözlemlenmiştir. EEPROM ve Flash belleklerde, kaydırma kapısı (floating-gate) yükü transistör hücresinin eşik voltaj değerini kaydırır, bu da okunan hücre değerinin duyu amplifikatörü ile tespit edilmesini sağlar. Veri kalıntısı problemi için kriptografik cihaz, genellikle sıcaklık sensörleri ve izinsiz girişi tespit eden dış müdahale sensörleri ile çevrili bir yapının içine sarılır. Böylece, gizli

anahtarı bellek içinden silmek için yeterli zaman sağlanır. Ancak düşük veri kalıntısına sahip gömülü bir SRAM tasarımı oldukça maliyetlidir çünkü bu SRAM hücrelerinin ilave imha sinyali dâhil edilerek değiştirilmesi anlamına gelir. Bir diğer kalıntı problemi üst üste silmedir (overerasing). Eğer silme döngüsü tekrar silinmiş bir hücreye uygulanırsa, kaydırma kapısının yük değeri pozitif kalır böylece bellek transistörü tüketme mod (depletion mode) transistöre çevrilir; bu da veri kalıntısına sebep olur.

10.2.3. Yarı Bozucu Saldırılar

Yarı bozucu saldırıların uygulanması için tıpkı bozucu saldırılar gibi çipin yüzeyine erişilmesi gerekir. Ancak çipin iç kısımları ile temas kurulmaz. Yarı bozucu saldırılar genellikle sistemi bozmaz, saldırının uygulanış şekline göre saldırı yapıldığına delil bırakabilir (aktif) veya bırakmaz (pasif). Aktif yarı bozucu saldırılarda temelde cihaza hata enjekte edilir. Pasif yarı bozucu saldırılarda okuma devreleri kullanılmadan veya derinlemesine araştırma yapılmadan bellekteki bilgilerin okunması sağlanır. Şekil 10.4'te bu saldırı adımlarında yapılan işlem aşamaları verilmiştir.



Şekil 10.4. Yarı Bozucu Saldırıların İşlem Aşamaları

Bu saldırılar, sistem ile yapılacak temasa göre masraflı olabilir ancak bozucu saldırılardan daha az masraflıdır. Bozucu saldırılar gibi çipin yüzeyine erişebilmek için öncelikle paketten çıkarma işlemi yapılır ancak pasivasyon tabakası bozulmadan kalır (çıkarılan katmanların ayrı ayrı işlenmesi işlemi

gerektirmez). Ayrıca metal yüzeye elektriksel erişim gerektirmez, bu nedenle silikonda herhangi bir mekanik tahribat olmaz. Daha sonra görüntüleme (imaging) işlemi yapılır. Bunun için kızılötesi (infrared) ışık kullanılarak çipin arka tarafından tarama yapılabilir. Bu saldırılar UV ışınları, X ışınları, lazer ışınları, elektromanyetik alan ve yerel ısıtma gibi farklı yöntemler kullanılarak gerçeklenebilir [5].

UV Işını Saldırıları önceleri bozucu saldırı olarak değerlendirilirken, bu saldırıların çoğu için sadece paketten çıkarma işlemi gerektiğinden yarı bozucu saldırı sınıfında değerlendirilmektedir [5]. Bu tür saldırılar OTP ve UV EPROM (EPROM UV ışınları ile silinebilir) gibi mikro-denetleyicilere kolayca uygulanabilir. Saldırı iki işlem adımına bölünür; sigortanın bulunması (finding fuse) ve UV ışınları ile sigortanın resetlenmesi. Güvenlik sigortası normalde program belleğinden daha erken silinemeyecek şekilde tasarlandığından, UV ışınları tüm çipe uygulanamaz. Bu nedenle bellek ışık geçirmez opak bir malzemeyle korunmalıdır, daha sonra UV ışını mikroskop veya lazer kullanılarak sigortaya uygulanabilir. Çip içinde sigortanın konumunun bulunması için çeşitli yöntemler mevcuttur. Bu yöntemlerden ilki, her ne kadar pahalı ve zaman alan bir yöntem olsa da tüm devre üzerinde tersine mühendislik yapmaktır. Kısmi tersine mühendislik kullanılarak zamandan tasarruf sağlanabilir. Bir diğer yöntem, çipin belirli kısımlarına zarar verip sonucu gözlemlemektir ancak bu işlem uzun sürebilir ve çok sayıda örneklem gerektirebilir. Eğer sigorta belleğe çok yakınsa veya gömülü ise konumlandırma çok zorlaşır. Sigortayı silmek için kullanılan UV ışını aynı zamanda sigortayı bulmak için de kullanılabilir. Bunun yanında UV ışınından korunacak bölgenin işaretlenmesi daha etkili ve ucuz yöntemlerden biridir. Diğer yarı bozucu saldırılar sigortayı bulmak için kullanılabilir. Şöyle ki; lazer tarama tekniği ile transistörlerin durumları direkt okunabildiğinden, bu yöntem sigortanın bulunmasında da kullanılabilir. Bir diğer yöntem ise optik hata enjekte yöntemidir, bu yöntemde çipin içinde yer alan farklı transistörlerin durumları değiştirilebilir ve sigorta durumunu etkileyecek konumlar bulunabilir [5].

İleri Görüntüleme saldırıları düşünüldüğünde, mikroskop altında görsel gözlemleme yapmak ilk adımdır. Ancak transistörlerin boyut özellikleri teknoloji geliştikçe küçüldüğünden, çip yüzeyinden bunları gözlemlemek daha da zorlaşmıştır. Bir diğer yöntem kızılötesi ışınların kullanılmasıdır ancak yüksek vernikli silikon devre levhaları kullanılan çipler kızılötesi ışınlara karşı daha

az şeffaf ve ışık kaynağına karşı daha hassastır. Görüntüleme saldırılarının bir diğer uygulaması ise ROM içerik çıkarımıdır. Kimyasal gravür baskı kullanılarak Mask ROM (Maskelenmiş ROM) içeriği çıkarılır, çıkarılan bu içerikten direkt gözlem yapılabilir. Bu saldırılar genellikle hata analiz aşamasında kullanılır [5].

Aktif Foton saldırıları ele alındığında, yarı iletken transistörler iyonlaştırıcı radyasyona karşı daha duyarlıdır. Bu nedenle 60'lı yıllarda iyonlaştırıcı radyasyonun yarı iletkenler üzerindeki etkilerini simüle etmek için lazerler kullanılmıştır. Kızılötesinden görünür ışığa geçerken, foton emilimi önemli oranda artar bu da modern çiplerde kırmızı ve yeşil lazerlerin uygulanabilir hâle gelmesini sağlamıştır. Aktif foton araştırmasında (problamada), taranan foton ışını çip ile etkileşime geçer. Enerjisi silikon bant boşluğundan daha büyük olan fotonlar yarı iletkende elektron deliği çiftleri üretir, enerjisi düşük olan fotonlar ise devre üzerindeki bağlantı noktalarıyla hâlâ etkileşime girebilir ancak tahribata yol açmayacak miktarda ısı ortaya çıkar. Foton kaynağı olarak lazer tarayıcı mikroskoplar kullanılır. Kırmızı düşük güçlü lazer ışıkları ile SRAM belleklerinin içeriği okunabilir. Bunun için öncelikle cihaz kapalı iken lazer ışıkları ile aktif alanlar iyonize edilerek belirlenir. Daha sonra cihaz açıkken yapılan taramada SRAM içeriği açık ve kapalı transistör kanalları görüntülenerek sızdırılabilir [5].

Optik hata oluşturma saldırılarında, devreye hata enjekte edilmesi amaçlanır. Örneğin bir transistör aydınlatılarak geçici bir arıza oluşturulabilir. Bu yöntemle SRAM belleklerde istenilen bit değiştirilebilir veya sıfırlanabilir. EPROM, EEPROM ve Flash gibi uçucu olmayan bellekler hata enjekte edilmeye karşı daha da hassastır. Sigorta tüpleri, üzerine ışık odaklanarak devre dışı bırakılabilir.

10.3. FİZİKSEL SALDIRI GÜVENLİK DEĞERLENDİRMELERİ VE ÖNLEMLERİ

Fiziksel saldırılardan korunmak için geliştirilen önlemler temelde, saldırı tespiti, saldırıyı önleyecek/zorlaştıracak karışıklıklar ekleme, önemli bilgileri maskeleme veya gizleme gibi yöntemler üzerine kuruludur. Bu önlemler detaylandırıldığında, bozucu, bozucu olmayan ve yarı bozucu saldırılara karşı alınabilecek önlemler aşağıda verildiği gibi alt başlıklarda sınıflandırılabilir.

10.3.1. Bozucu Saldırı Önlemleri

Veri yolu şifreleme (Bus Encryption), hassas bilgilerin elde edilmesini (problanmasını) önlemek için kullanılır. Bellek içerikleri CPU'ya gönderilmeden önce şifrelenir ve daha sonra CPU'ya ulaştığı zaman şifrelenen bellek içeriklerinin şifresi çözülür. Bu sayede CPU ile bellek arasındaki veri yolu içeriğine erişilse bile hassas bilgiler şifreli olduğu için korunur.

Veri yolu karıştırma (Bus Scrambling), saldırganın veri yolu bağlantılarını kullanarak fiziksel saldırı yapmasını önlemek amaçlı uygulanır. Veri yolu bağlantıları normalde sıralı bir şekilde bağlıdır. Ancak veri yolu karıştırma yöntemi uygulanarak veri yolları karışık şekilde bağlanır ve verinin takibi zorlaştırılır. Bu karıştırma işlemi statik, her mikro-denetleyici için farklı ve hatta her devre veya devre parçası için farklı şekilde uygulanabilir.

Sensör ağları (Sensor Mashes), derinlemesine araştırma saldırılarını tespit etmek amaçlı kullanılır. Cihazın en üst metal katmanındaki sensör ağı üzerindeki tüm yollar sürekli olarak izlenir ve herhangi bir derinlemesine araştırma denemesinde devre kısa devre olur ve alarm verir. Alarmdan sonra, belleklerdeki hassas verilerin korunması için bellek içeriği sıfırlanır. Bu önlemler, EBT (Electron Beam Testing–Elektron Demeti Testi) ve FIB sensör ağlarına karşı etkili bir şekilde kullanılabilirler.

Tümleşik devreler, ASIC (Application Specific Integrated Circuit - Uygulamaya Özel Tümleşik Devre) gibi özel tümleşik devrelerde; giriş/çıkış devreleri, talimat çözücüler, aritmetik ve mantıksal birimler gibi devre bileşenleri ayrı ayrı değil birbiri ile birleşik hâlde bulunur. Bu yapışık tasarım sayesinde veri yolları saklanmış olur. Bu sayede saldırganın saldıracak sinyali bulması imkânsız hâle gelir.

Farklı tipte sensörlerin kullanımı ile saldırılar yapıldığı esnada tespit edilebilir. Örneğin voltaj ve frekans sensörleri kullanılarak Hata Enjekte Saldırıları tespit edilebilir. Işık sensörleri, bozucu ve yarı bozucu saldırılarda uygulanan paketten çıkarma işlemini tespit edebilir. Ayrıca yüksek ve düşük ısı sensörleri, UV, kızılötesi, X-ray ve iyonize radyasyon sensörleri de kullanılabilir. Ancak sensörlerin çalışması için güç verilmesi gerekir. Dolayısıyla çalışmak için dışarıdan güç verilmesi gereken cihazlar için etkili bir yöntem değildir. Çünkü güç kapalı iken sensörler yok edilebilir. Bunlar dışında derinlemesine araştırma yapılabilmesi (problama) için özel amaçlı sensörler de geliştirilebilir.

Test devresinin yok edilmesi, cihazlar üretilirken test edilmesi için test devresi ile birlikte üretilir. Bazı saldırılar rastgele sinyaller yollayarak fabrika modu veya test moduna erişim sağlayabilir. Bunun önüne geçmek için cihaz son kullanıcıya sunulmadan önce test devresi fiziksel olarak yok edilerek güvenli hâle getirilmelidir.

10.3.2. Bozucu Olmayan Saldırı Önlemleri

Bozucu olmayan pasif yan kanal analizi saldırıları ele alındığında, bu saldırılara karşı alınacak önlemler Şekil 10.1'de sınıflandırıldığı gibi ayrı ayrı aşağıda verildiği gibi ele alınabilir.

Zamanlama analizi saldırıları için önlemler ele alındığında, saldırganın hedef aldığı mikromimari bileşenlerine göre farklı çözüm önerisi teknikleri sunulabilir. Bu teknikler sabit-zamanlı teknikler, gürültü enjekte (injecting noise), kararlılığı güçlendirme (enforcing determinism), zamanı bölme (partitioning time), donanımı bölme (partitioning hardware), denetleme (auditing) olarak sınıflandırılabilir [16]. Sabit-zamanlı tekniklerden kasıt, kriptografik kodu korumak için en genel yaklaşım, kodun davranışını veriden bağımsız olarak tasarlamaktır, ön bellek erişim veya dallanma dizileri örneğin anahtara veya açık metne bağlı olmamalıdır. Erişilen ön bellek satırlarının sırası gizli verilere bağlıysa, program ön bellekten bilgi sızdırabilir. Sabit-zamanlı kod yazım yöntemleri üzerine çalışmalara [39], [40], [41]'den erişilebilir. Sabit zamanlı yaklaşımın dezavantajı olarak bir donanım platformunda sabit zamanlı olan uygulamanın başka bir donanım platformunda sabit zamanlı olarak çalışmama olasılığı verilebilir. Bu nedenle sabit-zamanlı donanım işlemlerini sağlamak için komut setlerinde iyileştirmelere gidilmiştir [42]. Bunun yanında hem kod hem donanım tabanlı sabit-zamanlı koruma için, değişken olmayan yürütme uzunluğuna sahip özel dil semantiği geliştirilmesine yönelik çözümler önerilmiştir [43]. Gürültü enjeksiyonundaki amaç, zamanlama kanallarının içine saldırganın ölçümlerini önleyecek kadar çok gürültü ekleyerek kanalın sömürülmesini engellemektir. Rastgele arama tabloları ekleme, ön bellek indekslemesini rastgeleleştirme gibi işlemler zamanlama kanallarına gürültü eklenmesini sağlar [44], [45]. Kararlılığı (deterministliği) güçlendirme, zamanlama kanallarını ortadan kaldırmak, görünür zamanlama varyasyonlarını tamamen ortadan kaldırarak mümkündür düşüncesine dayanır. Bunun için iki yaklaşım vardır; sanal zaman (virtual time), diğeri siyah-kutu hafifletme (bla-

ck-box mitigation). Sanal zaman yaklaşımı, gerçek zamanlı erişimi tamamen ortadan kaldırmaya çalışır, ilerlemesi tamamen deterministik ve saldırıya açık bileşenlerin işlemlerinden bağımsız sanal saat vuruşları sağlar [46], [47]. Siyah-kutu hafifletme, gözlenebilir tüm saat vuruşlarını tek tek yürütülen işlemler ile senkronize etmeye çalışmak yerine, harici olarak görünür olayların zamanlamasını kontrol ederek bir bütün olarak sistemin determinize edilmesini sağlar [48], [49]. Zamanı bölme önlemi ile zamanlama kanallarından bilgi sızdırmadan zaman dilimleri arasındaki geçişi dikkatlice yönetmek amaçlanır. Bu önlem ön bellek temizleme (cache flushing) [46], kafes planlaması (Lattice scheduling) [50], minimum zaman dilimi (minimum timeslice) [51], bellek denetleyicisi bölümleme (memory controller partitioning) [52], çekirdek adres alanı yalıtımı (kernel address space isolation) [53] önlemlerini içerir. Donanımı bölme, donanım kaynaklarını çekirdek ve iş parçacıkları (threadler) arasında bölme işlemidir, bu sayede eş zamanlı zamanlama analizi saldırıları önlenebilir [16]. İş parçacıklarını devre dışı bırakma (disable hardware threading) [54], sayfa paylaşımını devre dışı bırakma (disable page sharing) [55], donanım ön bellek bölümleme (hardware cache partitions) [54], ön bellek renklendirme (cache colouring) [56] önlemleri donanımı bölme önlemleri arasında yer alır. Denetleme önlemleri temelde izleme sistemi kullanımına dayanır [57], [58].

Güç analizi saldırıları için önlemler, basit güç analizi, farksal güç analizi ve korelasyon güç analizi saldırıları için farklı olarak sınıflandırılabilir. Basit güç analizi için en temel önlem hesaplama prosedürlerinin gizli bilgiden bağımsız olmasıdır. Örneğin üs alma işlemi düşünüldüğünde bu saldırı, işlem yapılan gizli verilere bağlı üs alma sırasında meydana gelen güç tüketimi izlerini gözlemler. Eğer algoritmada kullanılan herhangi bir dallanma komutu gizli bilgiye bağlı ise bu güvenlik açığı ortaya çıkarır. Her üs alma işleminde güç tüketimi değiştirilmelidir. Bu nedenle dallanma komutunun kaldırılması veya algoritma içine ayırt edilemez toplama ve iki ile çarpma işlemleri eklenerek, üs alma algoritmasının tüm dallanma komutları gizlenir [59]. Ayrıca güç tüketiminin dengelenmesi için “dual rail” gibi teknikler kullanılabilir, şöyle ki düşük Hamming Ağırlığına sahip bir değerin (örneğin 0) manipülasyonu, diğer değerlerden birinin manipülasyonundan farklı bir güç tüketimine neden olmayacaktır [60]. Farksal güç analizi saldırıları için donanımsal önlemler ele alındığında; bu önlemler temelde varsayımsal güç tüketimi (hypothetical power consumption) ile cihazın güç tüketimi arasındaki korelasyonu azalt-

maya odaklanır. Varsayımsal güç tüketimleri saldırgan tarafından belirlenir, bu nedenle bir kriptosistemin tasarımcıları tarafından kontrol edilemez. Bu korelasyonu düşürmek için iki yaklaşım vardır; Sinyal Gürültü Oranı'nın (Signal-to-Noise Ratio-SNR) azaltılması, rastgele karıştırma yöntemlerinin kullanılması. SNR ne kadar düşük olursa, doğru varsayımsal güç tüketimi ile cihazın güç tüketimi arasındaki korelasyon da o kadar düşük olur. Güç tüketimi veri bağımlılığını azaltan özel mantık stillerinin kullanılması [61], çip üzerindeki kapasitansların rastgele doldurulması veya güç tüketiminin düzleştirilmesi (flattening), kriptografik algoritmanın çalışması sırasında paralel olarak çalışan herhangi bir işlem SNR'ın düşürülmesini sağlar. Rastgele karıştırma yöntemleri ise, rastgele gecikmelerin eklenmesi (yazılımsal önlem), deterministik olmayan işlemcilerin kullanılmasıdır [62]. Korelasyon güç analizi saldırıları, farksal güç analizi saldırılarının genişletilmiş hâli gibi düşünülebilir, bu nedenle bu saldırı yöntemine benzer şekilde sahte döngülerin eklenmesi, rastgele gecikmelerin eklenmesi, devre filtreleme veya gürültü ekleme ile güç izlerinin bulanıklaştırılması, veri-yolu şifreleme, veriyi rastgele bir sayı ile maskeleme önlemleri önerilebilir [25].

Elektromanyetik yayılım analizi saldırıları için alınabilecek önlemlerden bazıları, gizli bilgiyi bölme (secret splitting) [63], çoğaltma yöntemi (duplication method) [64], çarpımsal maskeleme (multiplicative masking) [65], rastgele maskeleme (random masking) [66] olarak verilebilir. Gizli bilgiyi bölme yönteminde, gizli bilgi küçük parçalara ayrılarak rastgele bir veri ile birleştirilir. Çoğaltma yönteminde ise, örneğin şifreleme algoritmasında karıştırmayı sağlayan S–kutusunun girdi değerleri gizli bilgi bölme yöntemiyle bölünür, sonrasında S–kutusu tabloları rastgele seçilmiş bir değer ile çoğaltılarak alternatif S–kutusu tablosu oluşturulur ve öncesinde bölünen S–kutusu girdileri bu alternatif tablodan geçirilir. Çarpımsal maskeleme ve rastgele maskeleme önlemleri ise, gizli bilginin her bir bitinin rastgele seçilmiş maskeleme bitleri ile sırasıyla çarpılması veya XORlama (exclusive-OR) işlemidir. Bunun yanında bölünmüş maske (split mask) önlemi ile S–kutusu çıktı değerleri rastgele seçilmiş farklı maske değeriyle maskelenir. Seçilen bu maskeleme değerleri maskeleme tablosunda tutulur [67]. Ayrıca Eşik Uygulaması (Threshold Implementation - TI) kullanılarak donanım platformlarında Boole maskelemesi gerçekleştirilir. TI, hataların varlığında bile sayısal devreler için güvenilir bir birinci dereceden maskeleme şemasıdır [68]. TI'ya alternatif olarak Etki Alanına Yönelik Maske-

leme (Domain - Oriented Masking - DOM) önerilmiştir. DOM'da daha az çip alanı ve daha az rastgelelikle TI ile aynı seviye güvenlik sağlanır [69]. Bunun yanında; devre çıkışına duyu amplifikatörü ekleme, parazit ekleme (jamming), dinamik uzamsal yer değiştirme ve haritalama, rastgele kontrol döngüsüne sahip voltaj regülatörü kullanımı, güç ızgaralarının (power grids) optimizasyonu (topolojinin veya iç direncinin modifiye edilmesi, ızgaralara kapasitör eklenmesi) elektromanyetik yayılımı önleyici yöntemlerdir [70].

Akustik analiz saldırısı için alınabilecek önlemler, ses geçirmez ekipmanların kullanımı, yeterince güçlü bir bant genişliğine sahip gürültü kaynağı kullanımı ile bilgilendirici sinyallerin maskelenmesi, kod içerisinde maskeleme ve normalizasyon işlemlerinin kullanılması, donanımın desteklediği frekans aralığının azaltılması, yan kanalların aktif olarak devre dışı bırakılması/parazit eklenmesi, hassas işlemlerin yürütüldüğü sırada ses sisteminin pasif hâle getirilmesi (mikrofon veya hoparlörden biri) olarak verilebilir [53], [71]. Parazit ekleme tekniğinde, bir cihaz akustik kanal faaliyetlerini izlemek üzere tasarlanabilir ve bir tehdit durumu algılandığında parazit eklemeyi etkinleştirebilir ya da yazılım ile hassas (gizli) işlemler yürütüldüğünde (mesela bir bankacılık uygulaması bir Kişisel Kimlik Numarası (Personal Identification Number–PIN) istediğinde) akustik kanalda aktif olarak parazit oluşturabilir.

Modern kriptosistemler kaba kuvvet saldırılarına karşı iki önemli önlemle geliştirilirler; hesaplama karmaşıklığını arttırma ve istatistiksel özellikler kullanılarak gizliliği koruma. Hesaplama karmaşıklığı yüksekse; saldırgan kriptosistemi polinomsal zamanda kıramaz. Hesaplama karmaşıklığı arttırarak gizli veriyi korumak için; ya anahtar uzunluğu arttırılır ya da Yalancı Rasgele Sayı Üreteçleri (Pseudo Random Number Generators–PRNGs) kullanılarak entropi arttırılır [54]. İstatistiksel özelliklerin kullanılarak gizli bilginin korunması temelde istatistiksel kodlama şemalarının tasarımına dayanır, literatürde farklı istatistiksel kodlama şeması tasarımları önerilmiştir [72], [73].

Hata oluşturma saldırıları için önlemler düşünüldüğünde, iki yaklaşım uygulanabilir; hatayı tespit etme, hata önleme. Hata tespiti için; hata girişimleri tespit edilir, kurtarma mekanizması izlenir, bilgi seviyesinde veri değişikliği algılanır. Hata önleme yaklaşımında ise çıktıyı bozma veya silme işlemleri uygulanır ancak maliyetlidir. Bu nedenle genellikle her iki yaklaşımın bir

kombinasyonu ile önlem oluşturulması beklenir. Yetersiz güç veya hız aşırtmayı izleyen, elektromanyetik tespitler yapan, gerçek zamanlı reaksiyon verebilecek uygun sensör ve dedektörlerin (lazer dedektörü, elektromanyetik alan dedektörü) kullanımı, hata tespit kodlarının uygulanması (veri bütünlüğünü sağlar), kopyalama (duplication) ve karşılaştırma işlemlerinin uygulanması (iki kez hesaplama, tersini hesaplama, yazılımın/donanımın kopyalanması), güç tüketimini dengeleyecek özel devrelerin (örneğin Dalga Dinamik Diferansiyel Mantık (Wave Dynamic Differential Logic – WDDL) devresi, Dengeli Hücre Tabanlı Çift Raylı Mantık (Balanced Cell-based Dual-rail Logic - BCDL) devresi [74]) kullanılması. Bunun yanında yazılım seviyesinde kopyalama, veri gösteriminin hatayı algılayacak şekilde değiştirilmesi, bazı hata modellerini destekleyen kodların yazılması, hata tespiti için makine dili seviyesinde kod analizörü tasarlama, akış kontrollerinin yapılması (önceden hesaplanmış imzaya karşı yürütülen kod imzasının doğrulanması), rastgeleleştirme (zamanın rastgeleleştirilmesi, rastgele titreşim ekleme, rastgele işlemler ekleme, rastgele karıştırma) önlemleri kullanılabilir [55] .

Veri kalıntısı saldırılarına karşı alınabilecek önlemler için, geliştiricilerin yarı iletken belleklerden veri kurtarmayı zorlaştırmaya yardımcı olan bazı genel tasarım kurallarına uymaları beklenir. EEPROM ve Flash bellekler için, yeni hücrelere gizli veriler saklanmadan önce, bu hücrelerin 10–100 kez rastgele veri ile doldurulması yeni hücrelerin kullanımı kaynaklı veri kalıntılarının ortadan kaldırılmasını sağlar. Tüm EEPROM ve Flash hücrelerinin silinmeden önce programlanması artık yük probleminin ortadan kaldırır. En yeni depolama aygıtlarının kullanılması, modern teknolojilerle tasarlanmış veya üstü metal katmanla kaplı belleklerin kullanılması veri kalıntısı saldırılarına bir önlemdir. Belleklere depolanacak verilerin şifrelenmesi bir diğer çözüm önerisidir [75].

10.3.3. Yarı Bozucu Saldırı Önlemleri

Yarı bozucu saldırılar birçok mikro-denetleyici için tehlikelidir. UV ışın saldırılarına karşı koruması olmayan mikro-denetleyicilerin güvenlik sigortası program belleğinden uzakta olduğundan, bu mikrodenetleyicilerin EPROM'u koli bandı gibi opak bir malzeme ile kaplanarak kolayca bozulabilir. Bu nedenle bazı firmalar güvenlik sigortalarını bellekle aynı sıraya yerleştirirler,

bu da ana belleği bozmadan sigortayı seçerek silmeyi zorlaştırır. Bunun yanında bazı firmalar güvenlik bitleri aktif olduğunda bellek içeriğini şifreleyen güvenlik korumaları kullanırlar. Ayrıca bazı mikro-denetleyicilerde devre sigortası opak üst metal tabaka ile kaplanır. Bazı firmalar ise UV ışınlarıyla resetlenmeyecek mikro-denetleyici üretmişlerdir [5]. Bunun yanında üretici firmalar çipe problar veya optik ışınlarla fiziksel erişimi önlemek için, çip yüzeyinin büyük kısımlarını kaplayan metal bir tabaka kullanırlar. Aktif Foton Problama saldırılarında lazerle tarama yapılmasını önleme amaçlı optik sensörler kullanılır. Bu sensörler cihazın fiziksel zayıflıklarını tespit etmeye ve lazer ışınlarını yakalamaya çalışır. Ayrıca bir cihazı yüksek voltajda çalıştırmak, bellek doğrulama tekniklerinin kullanılması, bellek karıştırma ve bellek şifreleme önlemleri Optik Hata Oluşturma Saldırılarına karşı başka çözüm önerileridir [76].

Tablo 10.2'de, bozucu, bozucu olmayan ve yarı bozucu saldırılara karşı donanımsal ve yazılımsal önlemler özetlenmiştir.

Tablo 10.2. Fiziksel Saldırılara Karşı Alınacak Önlemler

Saldırı Türü	Saldırı Sınıfı	Önlemler
Bozucu Saldırılar	Tersine Mühendislik Derinlemesine araştırma	- Veri yolu şifreleme, - Veri yolu karıştırma, - Sensör ağlarının kullanılması, - Farklı tipte sensörlerin kullanılması, - Test devresinin yok edilmesi
Bozucu Olmayan Saldırılar	Zamanlama Analizi (Yan Kanal saldırıları)	- Sabit-zamanlı yazılım/donanım tekniklerinin kullanılması, - Zamanlama kanalına gürültü enjekte edilmesi, - Deterministliği güçlendirme (sanal zaman, siyah-kutu hafifletme), - Zamanı bölme (ön bellek temizleme, Lattice planlaması, minimum zaman dilimi, bellek denetleyicisi bölümleme, çekirdek adres alanı yalıtımı), - Donanımı bölme (iş parçacıklarını devre dışı bırakma, sayfa paylaşımını devre dışı bırakma, donanım ön bellek bölümleme, ön bellek renklendirme), - Denetleme (izleme sistemlerinin kullanımı)
Bozucu Olmayan Saldırılar	Güç Analizi (Yan Kanal saldırıları)	- Hesaplama prosedürlerinin gizli bilgiden bağımsız olması, - Güç tüketimi dengeleme yöntemlerinin kullanılması, - SNR'ın azaltılması, - Rastgele karıştırma yöntemlerinin kullanılması, - Devre filtreleme, - Maskeleme, - Veri yolu şifreleme

Tablo 10.2. (Devam) Fiziksel Saldırılara Karşı Alınacak Önlemler

Bozucu Olmayan Saldırılar	Elektromanyetik Yayılım Analizi (Yan Kanal saldırıları)	- Gizli bilgiyi bölme, - Çoğaltma yöntemi, - Çarpımsal maskeleme, - Rastgele maskeleme, - Bölünmüş maske, - TI ile Boole maskeleme, - DOM maskeleme, - Devre çıkışına duyu amplifikatörü ekleme, - Parazit ekleme, - Dinamik uzamsal yer değiştirme ve haritalama, - Rastgele kontrol döngüsüne sahip voltaj regülatörü kullanımı, - Güç ızgaralarının optimizasyonu
Bozucu Olmayan Saldırılar	Akustik Analiz (Yan Kanal saldırıları)	- Ses geçirmez ekipmanların kullanımı, - Yeterince güçlü bir bant genişliğine sahip gürültü kaynağı kullanımı, - Maskeleme ve normalizasyon, - Donanımın desteklediği frekans aralığının azaltılması, - Yan kanalların aktif olarak devre dışı bırakılması / parazit eklenmesi
Bozucu Olmayan Saldırılar	Kaba Kuvvet Saldırıları	- Hesaplama karmaşıklığını arttırma önlemleri (anahtar uzunluğunu arttırma, PRNG kullanarak entropiyi arttırma), - İstatistiksel özellikleri kullanarak koruma sağlama
Bozucu Olmayan Saldırılar	Hata Oluşturma Saldırıları	- Sensör ve dedektörlerin (lazer dedektör, elektromanyetik dedektör) kullanımı, - Hata tespit kodlarının uygulanması, - Kopyalama ve karşılaştırma işlemlerinin uygulanması, - Güç tüketimini dengeleyecek özel devrelerin kullanılması, - Yazılım seviyesinde kopyalama, - Veri gösteriminin hatayı algılayacak şekilde değiştirilmesi, - Bazı hata modellerini destekleyen kodların yazılması, - Hata tespiti için makine dili seviyesinde kod analizörü tasarlama, - Akış kontrollerinin yapılması, - Rastgeleleştirme
Bozucu Olmayan Saldırılar	Veri Kalıntısı Saldırıları	- EEPROM ve Flash bellekler için yeni hücreler kullanılmadan önce bu hücrelerin rastgele veriyle doldurulması, - Tüm EEPROM ve Flash hücrelerinin silinmeden önce programlanması, - Modern teknolojilerin kullanılması, - Bellekte depolanacak verilerin şifreleme algoritmaları ile şifrelenmesi
Yarı Bozucu Saldırılar	UV Saldırıları İleri Görüntüleme Saldırıları Aktif Foton Problama Optik Hata Oluşturma Saldırıları	- Güvenlik sigortası ile belleğin birbirine yakın olması, - Belleğin karıştırılması ve şifrelenmesi, - Bellek doğrulama yöntemlerinin kullanılması, - Devre sigortasının metal tabaka ile kaplanması, - Optik sensörlerin kullanılması, - Cihazı yüksek voltajda çalıştırmak

10.4. SONUÇ VE DEĞERLENDİRMELER

Fiziksel saldırılar, kriptografik cihaz üzerinde yetkilendirme olmadan gizli bilgilerin elde edilmesini amaçlar. Bozucu, bozucu olmayan ve yarı bozucu saldırılar olarak gruplandırılırlar.

- Bozucu saldırılar; pahalı ekipmanlar, uzman kişiler ve zaman gerektirir. Saldırı sonrasında kanıt bırakılır veya cihaz yok edilir. Saldırı için gerekli ekipmanlar; lehimleme/sökme istasyonu, basit kimyasal laboratuvar, yüksek çözünürlüklü optik mikroskop, tel yapıştırma makinesi, lazer kesim sistemi, derinlemesine araştırma istasyonu, osiloskop, mantık analizörü, sinyal üreteci, elektron mikroskop tarayıcısı, FIB iş istasyonlarıdır.
- Bozucu olmayan saldırılar; düşük maliyetlidir, kriptografik cihaza fiziksel bir tahribat yapılmadan cihaz hareketleri gözlemlenir veya manipüle edilir. Çok maliyetli olmayan ekipmanlar ve orta derecede uzmanlık bilgisi gerektirir, normalde saldırı sonrası herhangi bir tahribat kanıtı bırakılmaz. Saldırı için kullanılan araçlar lehimleme/sökme istasyonu, dijital ölçü aleti, test cihazları, güç kaynakları, osiloskop, mantık analizörü, sinyal üreteç, veri toplama kartları olarak verilebilir.
- Yarı bozucu saldırılar; hedef cihaza daha az zarar verirler, diğer bir ifadeyle sadece paketten çıkarma işlemi yapılır. Bozucu saldırılara göre daha ucuz ve kurulumu kolaydır. Saldırı sırasında kullanılan ekipmanlar; lehim/sökme istasyonu, basit kimyasal laboratuvar, yüksek çözünürlüklü optik mikroskop, UV kaynakları, lazerler, özel mikroskoplar (lazer tarama, kızılötesi mikroskop), osiloskop, mantık analizörü, sinyal üreteci, veri toplama kartları, prototip panolardır.

Bu bölümde her bir fiziksel saldırı sınıfı kapsamlı olarak ele alınmış ve bu saldırılara karşı alınması gereken önlemler alt bölümlere ayrılarak detaylandırılmıştır. Tamamen mükemmel koruma sağlayan bir kriptosistem tasarım örneği yoktur çünkü bir saldırgana yeterli zaman ve kaynak verildiğinde kriptosistem kırılabilir. Ancak bu kriptosistemin saldırılara karşı tamamen savunmasız olduğu anlamına gelmez. Bunun yanında, sadece bir saldırı sınıfına yönelik önlemin alınması kriptosistemi fiziksel saldırıların tümünden korumaz; bu nedenle kriptosistem mümkün olduğunca çok önlem içerecek şekilde tasarlanmalıdır.

Teşekkür

Çalışmada, Meltem Kurt Pehlivanoğlu TÜBİTAK 2219-Yurt Dışı Doktora Sonrası Araştırma Burs Programı kapsamında kısmi olarak desteklenmiştir.

KAYNAKLAR

[1] M. Cenk, Siber Güvenlikte Kriptografi, Kriptografik Test Yöntemleri Ve Kriptoanaliz, Siber Güvenlik ve Savunma: Problemler ve Çözümler, pp. 63-83, 2019.

[2] M.T. Sakallı, Kriptografik Test Yöntemleri Ve Kriptoanaliz, Siber Güvenlik ve Savunma: Problemler ve Çözümler, pp. 87-134, 2019.

[3] N. Çaydaş, Yan Kanal ve Hata Yaptırma Atak Cihazlarının Hazırlanan Test Yazılımı ile Yönetilmesi ve Alınan Ölçümlerin Analiz Edilmesi, Yükesk Lisans Tezi, İstanbul Şehir Üniversitesi, İstanbul, Türkiye, 2019.

[4] FX. Standaert, Introduction to Side-Channel Attacks. In: Secure Integrated Circuits and Systems, pp. 27–42, Springer, 2010.

[5] S.P. Skorobogatov, Semi-Invasive Attacks - A New Approach to Hardware Security Analysis, Technical Report UCAM-CL-TR-630, University of Cambridge Computer Laboratory, 2005.

[6] P. Kocher, Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and Other Systems, CRYPTO'96, LNCS, Vol. 1109, pp. 104-113, 1996.

[7] P. Kocher, J. Jaffe, B. Jun, Differential Power Analysis, CRYPTO'99, LNCS, Vol. 1666, pp. 398-412, 1999.

[8] D. Agrawal, B. Archambeault, J. Rao, P. Rohatgi, The EM Side-Channel(s), CHES'02, LNCS, Vol. 2523, pp. 29-45, 2002.

[9] J. Di-Battista, JC. Courrege, B. Rouzeyre, L. Torres, P. Perdu, When Failure Analysis Meets Side-Channel Attacks, CHES'10, LNCS, Vol. 6225, pp. 188-202, 2010.

[10] G.M. Deepa, G. Sriteja, S. Venkateswarlu, An Overview of Acoustic Side-Channel Attack, International Journal of Computer Science & Communication Networks, Vol. 3, No. 1, pp. 15-20, 2013.

[11] F. Koeune, FX. Standaert, A Tutorial on Physical Security and Side-Channel Attacks, FOSAD'05, LNCS, Vol. 3655, pp. 78-108, 2005.

[12] Y. Lyu, P. Mishra, A Survey of Side-Channel Attacks on Caches and Countermeasures, Journal of Hardware and Systems Security, Vol. 2, pp. 33-50, 2018.

[13] N. Tsalis, E. Vasilellis, D. Mentzelioti, T. Apostolopoulos, A Taxonomy of Side Channel Attacks on Critical Infrastructures and Relevant Systems, Critical Infrastructure Security and Resilience, Advanced Sciences and Technologies for Security Applications. Springer, pp. 283-313, 2019.

[14] A. Golder, D. Das, J. Danial, S. Ghosh, S. Sen, A. Raychowdhury, Practical Approaches Toward Deep-Learning-Based Cross-Device Power Side-Channel Attack, IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 27, No. 12, pp. 2720-2733, 2019.

[15] F. Kenarangi, I. Partin-Vaisband, Exploiting Machine Learning Against On-Chip Power Analysis Attacks: Tradeoffs and Design Considerations, IEEE Transactions on Circuits and Systems–I, Vol. 66, No. 2, pp. 769-781, 2019.

[16] Q. Ge, Y. Yarom, D. Cock, G. Heiser, A Survey of Microarchitectural Timing Attacks and Countermeasures on Contemporary Hardware, J Cryptogr Eng, Vol. 8, pp. 1–27, 2018.

[17] J. C. Wray, An Analysis of Covert Timing Channels, IEEE Computer Society Symposium on Research in Security and Privacy, pp. 2–7, 1991.

[18] J. F. Dhem, F. Koeune, PA. Leroux, P. Mestré, J.-J. Quisquater, JL. Willems, A Practical Implementation of the Timing Attack, CARDIS'98. LNCS, Vol. 1820, pp. 167-182, 1998.

[19] D. Mayer, J. Sandin, Time Trial: Racing Towards Practical Timing Attacks, Matasano Security Research, 2014, available at: https://www.nccgroup.trust/uk/our-research/?style=Cyber%20Security%202.

[20] Y. Yarom, Microarchitectural Side-Channel Attacks, 2016, available at: https://www.iacr.org/workshops/ches/ches2016/presentations/CHES16-Tutorial2_1.pdf.

[21] D. Gruss, Software-based Microarchitectural Attacks, Ph. D. Thesis, Institute for Applied Information Processing and Communications Graz University of Technology, Graz, Austria, 2017.

[22] D. J. Bernstein, Cache-timing attacks on AES, Technical Report, Department of Mathematics, Statistics, and Computer Science, University of Illinois, 2005.

[23] J. Bonneau, I. Mironov, Cache-Collision Timing Attacks Against AES, CHES 2006, LNCS, Vol. 4249, pp. 201-215, 2006.

[24] L. Ordu, S.B. Örs Yalçın, Yan-Kanal Analizi Saldırılarına Genel Bakış, Ulusal Elektronik İmza Sempozyumu, pp. 1–8, 2006.

[25] E. Brier, C. Clavier, F. Olivier, Correlation Power Analysis with a Leakage Model, CHES'04, LNCS, Vol. 3156, pp. 16–29, 2004.

[26] E. Peeters, FX. Standaert, J.J. Quisquater, Power and Electromagnetic Analysis: Improved Model, Consequences and Comparisons, Integration the VLSI Journal, Vol. 40, No. 1, pp. 52–60, 2007.

[27] A. Sayakkara, NA. Le-Khac, M. Scanlon, A Survey of Electromagnetic Side-Channel Attacks and Discussion on Their Case-Progressing Potential for Digital Forensics, Digital Investigation, Vol. 29, pp. 43-54, 2019.

[28] R. Callan, A. Zaji´c, M. Prvulovic, FASE: Finding Amplitude Modulated Side-channel Emanations, ACM SIGARCH Computer Architecture News, Vol. 43, ACM, 2015, pp. 592– 603, 2015.

[29] M. Prvulovic, A. Zaji´c, R. L. Callan, C. J. Wang, A Method for Finding Frequency-modulated and Amplitude-modulated Electromagnetic Emanations in Computer Systems, IEEE Transactions on Electromagnetic Compatibility, Vol. 59, No. 1, pp. 34–42, 2017.

[30] G. Camurati, S. Poeplau, M. Muench, T. Hayes, A. Francillon, Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers, Proceedings of the 25th ACM Conference on Computer and Communications Security, 2018.

[31] M. Backes, M. Dürmuth, S. Gerling, M. Pinkal, C. Sporleder, Acoustic Side-channel Attacks on Printers, Proceedings of the USENIX Security'10, 2010.

[32] A. Faruque, M. Abdullah, S.R. Chhetri, A. Canedo, J. Wan, Acoustic Side-channel Attacks on Additive Manufacturing Systems, Proceedings of the ICCPS'16, 2016.

[33] E. Toreini, B. Randell, F. Hao, An Acoustic Side Channel Attack on Enigma, Computing Science Technical Report, Newcastle University, 2015.

[34] S. Narain, A. Sanatinia, G. Noubir, Single-stroke Languageagnostic Keylogging Using Stereo-microphones and Domain Specific Machine Learning, WiSec'14, 2014.

[35] P. Cheng, I.E. Bagci, U. Roedig, J. Yan, SonarSnoop: Active Acoustic Side-channel Attacks, International Journal of Information Security, 2019, available at: https://doi.org/10.1007/s10207-019-00449-8.

[36] H-J. Jo, J.W. Yoon, A New Countermeasure Against Brute-Force Attacks That Use High Performance Computers for Big Data Analysis, International Journal of Distributed Sensor Networks, Vol. 2015, pp. 1– 7, 2015.

[37] S. Bhasin, D. Mukhopadhyay, Fault Injection Attacks: Attack Methodologies, Injection Techniques and Protection Mechanisms, Security, Privacy, and Applied Cryptography Engineering SPACE'16, LNCS, Vol. 10076, pp. 415– 418, 2016.

[38] P. Gutmann, Secure Deletion of Data from Magnetic and Solid-State Memory, 6th USENIX Security Symposium Proceedings, pp. 77–89, 1996.

[39] B. Köpf, L. Mauborgne, M. Ochoa, Automatic Quantification of Cache Side-channels, Proceedings of the 24th International Conference on Computer Aided Verification, pp. 564–580, 2012.

[40] G. Doychev, B. Köpf, L. Mauborgne, J. Reineke, CacheAudit: A Tool for the Static Analysis of Cache Side Channels, ACM Trans. Inf. Syst. Secur, Vol. 18, No. 1 No. 1, 2015.

[41] A. Rane, C. Lin, M. Tiwari, Secure, Precise, and Fast Floatingpoint Operations on x86 Processors, Proceedings of the 25th USENIX Security Symposium, 2016.

[42] D. Page, Defending Against Cache-based Side-channel Attacks, Inf. Secur. Tech. Rep., Vol. 8, No. 1, pp. 30–44, 2003.

[43] D. Zhang, A. Askarov, A.C. Myers, Language-based Control and Mitigation of Timing Channels, Proceedings of the 2012 ACM SIGPLAN Conference on Programming Language Design and Implementation, pp. 99–110, 2012.

[44] E. Brickell, G., Graunke, M. Neve, J.-P. Seifert, Software Mitigations to Hedge AES Against Cache-based Software Side Channel Vulnerabilities, IACR Cryptology ePrint Archive, 2006.

[45] Z. Wang, R.B. Lee, New Cache Designs for Thwarting Software Cache-based Side Channel Attacks, 34th International Symposium on Computer Architecture, 2007.

[46] P. Li, D. Gao, M.K. Reiter, Mitigating Access-driven Timing Channels in Clouds Using StopWatch, 43rd International Conference on Dependable Systems and Networks (DSN), pp. 1–12, 2013.

[47] W. Wu, E. Zhai, D. Jackowitz, D.I. Wolinsky, L. Gu, B. Ford, Warding Off Timing Attacks in Deterland. arXiv preprint arXiv:1504.07070, 2015.

[48] B. Köpf, M. Dürmuth, A Provably Secure and Efficient Countermeasure Against Timing Attacks, 22nd IEEE Computer Security Foundations Symposium, pp. 324–335, 2009.

[49] B.A. Braun, S. Jana, D. Boneh, Robust and Efficient Elimination of Cache and Timing Side Channels, arXiv preprint arXiv:1506.00189, 2015.

[50] D. Cock, Practical Probability: Applying pGCL to Lattice Scheduling, 4th International Conference on Interactive Theorem Proving, pp. 1–16, 2013.

[51] V. Varadarajan, T. Ristenpart, M. Swift, Scheduler-based Defenses Against Cross-VM Side-channels, 23rd USENIX Security Symposium, 2014.

[52] Y. Wang, A. Ferraiuolo, G.E. Suh, Timing Channel Protection for a Shared Memory Controller, 20th IEEE Symposium on High-Performance Computer Architecture, 2014.

[53] D. Gruss, C. Maurice, A. Fogh, M. Lipp, S. Mangard, Prefetch Side-channel Attacks: Bypassing SMAP and Kernel ASLR, 23rd ACM Conference on Computer and Communications Security, 2016.

[54] C. Percival, Cache Missing for Fun and Profit, BSDCan'05, 2005.

[55] Z. Zhou, M.K. Reiter, Y. Zhang, A Software Approach to Defeating Side Channels in Last-level Caches, 23rd ACM Conference on Computer and Communications Security, 2016.

[56] J. Shi, X. Song, H. Chen, B. Zang, Limiting Cache-based Sidechannel in Multi-tenant Cloud Using Dynamic Page Coloring, International Conference on Dependable Systems and Networks Workshops (DSN-W), pp. 194–199, 2011.

[57] L. Fiorin, G. Palermo, C. Silvano, A Security Monitoring Service for NoCs, 6th International Conference on Hardware/Software Codesign and System Synthesis, pp. 197– 202, 2008.

[58] T. Zhang, Y. Zhang, R.B. Lee, Memory DoS Attacks in Multi-tenant Clouds, Severity and Mitigation. arXiv preprint arXiv:1603.03404v2, 2016.

[59] H. Mamiya, A. Miyaji, H. Morimoto, Efficient Countermeasures Against RPA, DPA, and SPA, CHES'04. LNCS, Vol. 3156. pp. 343–356, 2004.

[60] J.C. Courrège, B. Feix, M. Roussellet, Simple Power Analysis on Exponentiation Revisited, Smart Card Research and Advanced Application CARDIS'10, LNCS, Vol. 6035, 2010.

[61] S. Moore, R. Anderson, P. Cunningham, R. Mullins, G. Taylor, Improving Smart Card Security using Self-timed Circuits, Eighth IEEE International Symposium on Asynchronous Circuits and Systems – Async'02, 2002.

[62] S. Mangard, Hardware Countermeasures against DPA – A Statistical Analysis of Their Effectiveness, Topics in Cryptology – CT-RSA 2004, LNCS, Vol. 2964. pp. 222-235, 2004.

[63] S. Chari, C.S. Jutla, J.R. Rao, P. Rohatgi, Towards Sound Approaches to Counteract Power-Analysis Attacks, CRYPTO'99, LNCS, Vol. 1666, pp. 398– 412, 1999.

[64] L. Goubin, J. Patarin, DES and Differential Power Analysis The "Duplication" Method, CHES'99, LNCS, Vol. 1717, pp. 158– 172, 1999.

[65] J.D. Golić, C. Tymen, Multiplicative Masking and Power Analysis of AES, CHES'02, LNCS, Vol. 2523, pp. 198– 212, 2003.

[66] T.S. Messerges, Securing the AES Finalists Against Power Analysis Attacks, FSE '00, LNCS, Vol. 1978, pp. 150– 164, 2001.

[67] Catherine H. Gebotys ve C. C. Tiu ve X. Chen, A Countermeasure for EM Attack of a Wireless PDA, International Symposium on Information Technology: Coding and Computing ITCC'05, pp. 544–549, 2005.

[68] S. Nikova, V. Rijmen, M. Schlaffer, Secure hardware implementation of nonlinear functions in the presence of glitches, J. Cryptology, Vol. 24, No. 2, pp. 292–321, 2011.

[69] H. Gross, S. Mangard, T. Korak, Domain-oriented masking: compact masked hardware implementations with arbitrary protection order, Cryptology ePrint Archive, Report 2016/486, 2016.

[70] C. Wang, Y. Cai, H. Wang ve Q. Zhou, Electromagnetic Equalizer: An Active Countermeasure Against EM Side-channel Attack, 2018 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), pp. 1-8, 2018.

[71] E. Tromer, Hardware –Based Cryptanalysis, Ph. D. Thesis, Weizmann Institute of Science, Rehovot, Israel, 2007.

[72] H-J. Jo ve J. W. Yoon, Poster: Statistical Coding Scheme for the Protection of Cryptographic Systems Against Brute-force Attack, in Proceedings of the 35th IEEE Symposium on Security and Privacy, 2014.

[73] A. Juels, T. Ristenpart, Honey Encryption: Security Beyond the Brute-force Bound, in Advances in Cryptology— EUROCRYPT'14, Vol. 8441, LNCS, pp. 293–310, 2014.

[74] M. Nassar, S. Bhasin, J. L. Danger, G. Duc, S. Guilley, BCDL: A high performance balanced DPL with global precharge and without early-evaluation, DATE'10, pp. 849–854, 2010.

[75] S. Skorobogatov, Data Remanence in Flash Memory Devices, CHES 2005, Vol. 3659, LNCS, pp. 339–353, 2005.

[76] S. Skorobogatov, Optical Fault Masking Attacks, Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), pp. 23–29, 2010.

Bölüm 11

KÜRESEL SALGININ ULUSAL BİLİŞİM GÜVENLİĞİNE ETKİLERİ

Ensar Şeker

Tüm dünyayı derinden etkileyen ve Dünya Sağlık Örgütü (DSÖ) tarafından pandemi olarak ilan edilen COVID-19 salgını beklenmedik bir biçimde hayatlarımızı etkilemiş ve önemli değişikliklere neden olmuştur. Salgın sürecinde siber uzayda da yakından takip ve analiz edilmesi gereken olaylar zinciri birbirini izlemiştir. Bu kitap bölümde krizi bir fırsata çevirmeye çalışan siber korsanların taktik, teknik ve stratejileri rakamlarla analiz edilerek bir sonraki krizden önce atılması gereken adımlar bu analizlere dayandırılarak sunulmuştur.

11.1. GİRİŞ

Ne yazık ki, COVID-19 dünya çapında bir felakete sebebiyet verirken siber saldırılarda da keskin bir artışa yol açmıştır. Siber suçlular mevcut durumdan hızlı bir şekilde faydalanmak için vakit kaybetmeden harekete geçmiş, hastane gibi sağlık sektöründeki hizmet sağlayıcıların yanı sıra imalat ve ilaç endüstrilerindeki işletmeleri ve hatta kamu yetkililerini hedef almışlardır. Bu saldırılar bu sektörlerle sınırlı kalmayarak kısa zaman içerisinde tüm sektörleri hatta bireysel internet kullanıcıları dahi hedef alacak bir biçimde yaygınlaşmıştır.

Sadece bu yılın Mart ayında, çeşitli endüstrilerdeki kuruluşlar kötücül amaçlı yazılım saldırılarında %475 artış bildirmişlerdir.

Saldırılar, sahte bir Dünya Sağlık Örgütü (DSÖ) mobil uygulamasında yerleşik bilgi çalan kötücül amaçlı yazılımlar, oltalama e-postalar ile kimlik hırsızlığı, karanlık internet (darkweb) üzerinden yüz maskeleri, el dezenfektanı, sahte COVID-19 test kitleri ve virüs için sahte tedavi ilaçları satışı gibi oldukça geniş bir perspektifte gerçekleştirmişlerdir.

Saldırıların çeşitliliği ve saldırı alanlarının artışının en önemli nedenlerinden biri de hiç şüphesiz pandemi döneminde uzaktan çalışma iş modeline, yeni çalışma düzenlerine geçilmesidir.

11.2. YENİ ÇALIŞMA DÜZENİ: UZAKTAN İŞ GÜCÜ

2019 yılının son aylarında ortaya çıkan ve pandemi ilanına sebep olan COVID-19 virüsü ve beraberinde getirdiği felaketler şirketler ve çalışanlar için günlük normların aniden değişmesine ve iş yaşamı ile birlikte tüm hayatın derinden etkilenmesine yol açtı. Birçok şirketin İş Sürekliliği Planları ya mevcut değildi ya da bu planları tüm iş gücü ve operasyonları ile birlikte uygulamaya hazırlıklı değildiler. Pandeminin yayılmasının önüne geçebilmek için tüm dünyada sıkı tedbirler birer birer uygulanmaya başlarken gündelik operasyonların ve iş sürekliliğin devamı için çalışanların uzaktan iş gücüne katkı sağlayabilmesi için yeni yöntem ve metotlar uygulanmaya başlandı. Bunlar arasında toplantı ve görüşmelerin çevrimiçi ortamlarda telekonferans çözümleri ile gerçekleştirilmesi, verilere kolay erişim sağlanabilmesi için bulut tabanlı alt yapıların kullanılması, gizlilik dereceli verilerin korunabilmesi için VPN tabanlı teknolojilerin adapte edilmesi gibi örnekler sıralanabilir.

Bu yeni çalışma düzenine belki de en çabuk siber saldırganlar adapte oldu ve bu süreçte kullanımı artan bu uygulamaların zafiyetlerini sömürmek için yeni stratejiler geliştirdiler. Bu durum kişiler ve organizasyonlar için ciddi tehditler doğururken ulusal bilişim güvenliğini tehdit eden hususlar da ciddi bir boyuta ulaşmıştır.

11.3. PANDEMİ VE BİLGİ GÜVENLİĞİ

Bilgi güvenliği politikalarının saç ayaklarını gizlilik (confidentiality), bütünlük (integrity) ve erişilebilirlik (availability) oluşturmaktadır [1]. Bilgi güvenliği uzmanları, bir kişi, kurum ya da kuruluşun kişisel olarak tanımlanabilir bilgileri ile hassas bilgi ve verilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini güvence altına almak için çalışır. Bilgisayar korsanları, basit komut dosyaları çalıştıran (script kiddies) alt seviyeden gelişmiş kalıcı tehdit (APT) ve siber silahlar geliştiren üst seviye gruplara kadar beceri, finansman ve nihai hedef olarak çeşitlilik gösterir. Açık kaynak araçlarını indirebilen ve temel komut dosyası saldırılarını kolayca gerçekleştirebilen, genelde kişisel tatmin ya da politik amaçlı saldırılar yapan saldırganlardan ekonomik gelir elde etmek ve daha da ileri seviyede genellikle ulus-devlet destekli çok fazla finansman desteği olan, onlarca yıllık deneyimi ve ileri seviye ekipmanlara sahip imkânlarını uluslararası casusluk ve siber savaş için kullanan APT gruplarının ulaşmak istedikleri hedefler birbirinden oldukça farklıdır.

Bununla birlikte kriz anları genellikle siber saldırılarda ve güvenlik ihlallerinde bir artışa neden olur. Siber suçluların dolandırıcılık, kimlik hırsızlığı ve sosyal mühendislik yoluyla kredi kartı verileri de dâhil olmak üzere birçok özel ve gizli bilgileri çalmak için krizden faydalandığı COVID-19 salgını döneminde de gözlemlenmiştir.

11.4. COVID-19 SALGININ ORTASINDA SİBER TEHDİTLER

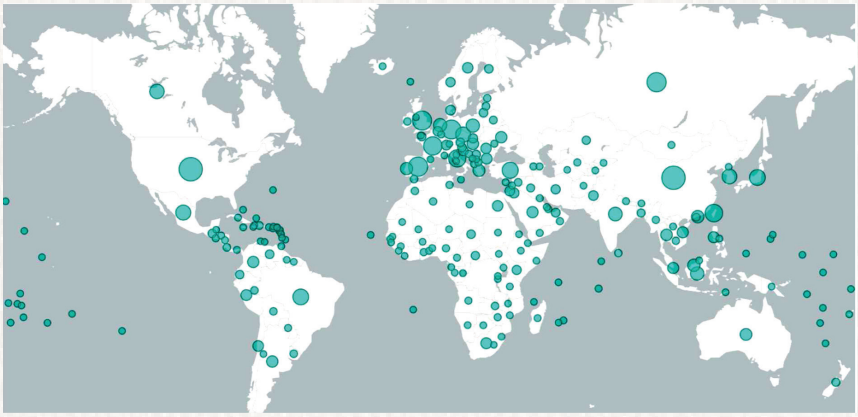
Koronavirüsün yayılmasına, uzaktan çalışanlar, devlet kurumları ile ulusal ve uluslararası tıbbi tesislere karşı siber saldırılar da daha fazla bir artışla eşlik etmiştir. Tehditlerin sayısı ve etkisinin artmasıyla birlikte istihbarat, ulusal güvenlik ve kolluk kuvvetleri tarafından daha fazla uyarların ciddiyeti ile uyarı sayısı arttırılırken, bu kapsamda dikkate değer önlemler alınmaya başlanmıştır.

ABD ve İngiltere'nin ilgili siber güvenlik birimleri tarafından yayınlanan ortak bir bildirgede kriz ortamını fırsata çevirmek isteyen bilgisayar korsanlarının faaliyetlerine dikkat çekilmiştir. Bu faaliyetler arasında sahte video konferans ve uzaktan erişim uygulamaları aracılığıyla kötü amaçlı yazılımları dağıtmanın

yanı sıra dijital kimlik avı ve fidye yazılımı saldırılarının pandemi sürecindeki artışına özellikle vurgu yapılmıştır. Yine son zamanlarda, FBI ve Interpol, devlet destekli bilgisayar korsanları ve COVID-19 ile ilgili araştırmaya açıkça katıldıklarını belirten tıbbi kurumları hedef alan fidye yazılımı saldırıları ile siber casusluk operasyonlarına karşı uyaran tavsiyeler yayınlamışlardır. NASA tarafından çalışanlarına bu süreçteki saldırılarla ilgili bilgiler aktarılarak dâhilî uyarılar yapıldığı bildirilmiştir. FBI ve Hindistan'ın ulusal siber olaylara müdahale (USOM) ekibine göre kötü niyetli aktörler çevrimiçi okul derslerini kesintiye uğratmış ve bu kayıtlardaki kişisel verileri toplamışlardır. Uyarılara yanıt olarak, birçok devlet kurumu ve küresel şirket Google, SpaceX, ABD Senatosu, Tayvan hükümeti, Alman Dışişleri Bakanlığı ve Avustralya Savunma Bakanlığı dâhil olmak üzere birçok güvenlik sınırlamalarını faaliyete geçirmiş ve bu kapsamda birçok uygulamanın kullanımını da yasaklamıştır.

Bu süreçte siber casusluk operasyonlarını da artış gösterdiği gözlemlenmiştir. Örneğin Çin, devlet kurumlarını COVID-19 ile ilgili bilgiler arayışında hedefleyen Vietnamlı bir siber casusluk kampanyası tespit ettiğini duyurdu. Google'ın Tehdit Analizi Grubu, sağlık kuruluşlarını hedef alan bir düzineden fazla devlet destekli saldırgan (hacker) grubu hakkında bulguları olduğunu duyurdu. Aynı zamanda, bazı devlet destekli saldırgan grupları sosyal medya üzerinden dezenformasyon kampanyaları başlattılar.

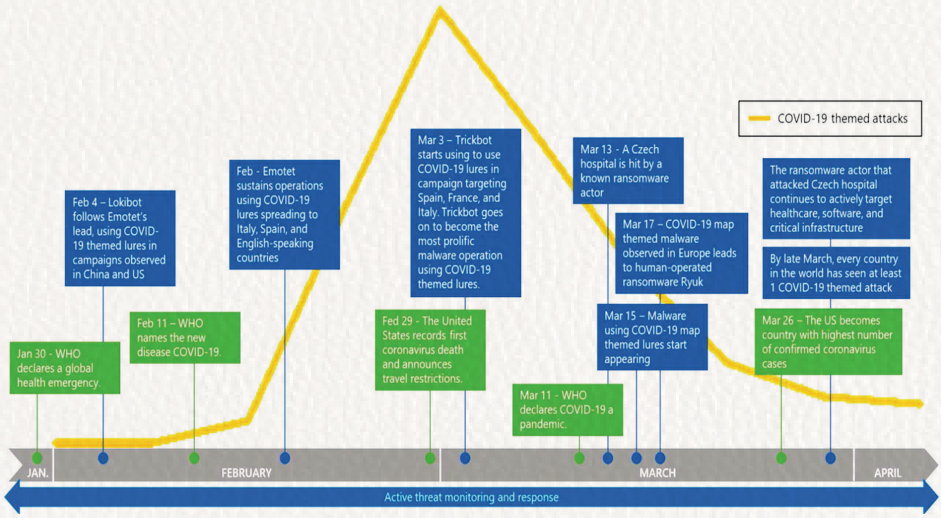
COVID-19 temalı saldırılar analiz edildiğinde aşağıdaki sonuçları yorumlamak mümkündür;



Şekil 11.1. COVID-19 Temalı Siber Saldırıların Dünya Genelinde Dağılımı ve Etkisi (7 Nisan 2020 itibariyle)

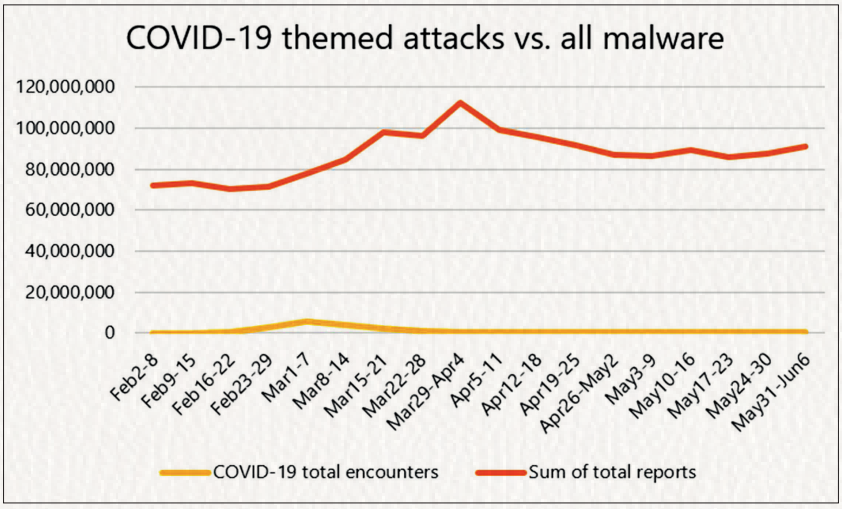
Dünyadaki her ülke en az bir COVID-19 temalı saldırı görmüştür (bkz. Şekil 11.1) [2]. Salgın isabet eden ülkelerde başarılı saldırıların hacmi, korku ve bilgi arzusu büyüdükçe artmaktadır. Çin, ABD ve Rusya'nın en ağır darbeye maruz kalmıştır.

Yaygın kullanıma sahip Trickbot ve Emotet kötü amaçlı yazılım aileleri çok aktif olarak kendilerine yer edinmeye başlamış ve salgından yararlanmak için cazibelerini yeniden markalandırma çalışmalarına girmişlerdir. COVID-19 temalı oltalama saldırıları kullanılarak küresel çapta bugüne kadar 76 tehdit varyantı gözlemlenmiştir.60 binden fazla COVID-19 temalı eklenti ve kötücül URL tespit edilmiştir. COVID-19 temalı siber saldırılar Mart ayının ilk iki haftasında zirveye ulaştı. Ulusal bilişim güvenliğinden sorumlu birimlerin tehditler için karşı tedbirler geliştirmesi ve uyarılarını yaygınlaştırılması ile saldırıların seyrinde bir takım değişiklikler oldu.



Şekil 11.2. COVID-19 Temalı Siber Saldırılarda Eğilimler

Siber saldırılardaki bu değişimler küresel tehdit ortamı için tipik bir dalgalanma seyri göstermektedir. Bununla birlikte krizin küresel doğası ve evrensel etkisinin siber suçluların çalışmasını nasıl kolaylaştırdığı analizler sonucu çok net bir şekilde gözükmektedir [3].

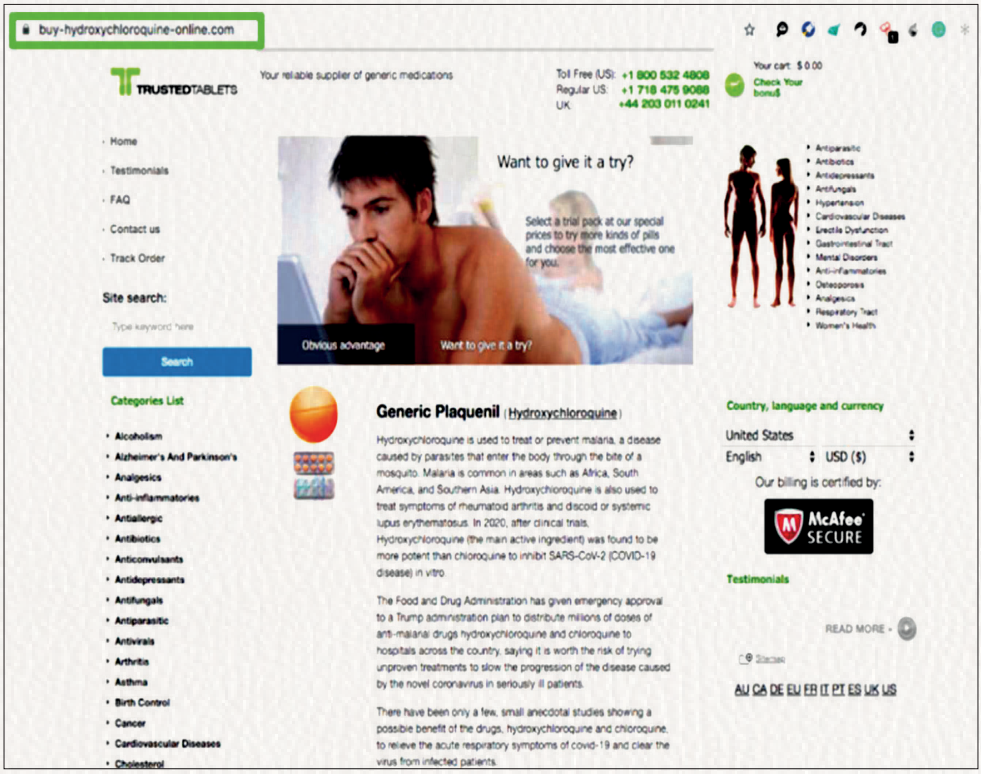


Şekil 11.3. Küresel Siber Saldırıların COVID-19 Siber Saldırıları ile Kıyaslanması

Siber korsanların taktik, teknik ve stratejileri şekil 11.4'te [4] daha kapsamlı bir şekilde gözlemlenebilmektedir.

Şekil 11.4. COVID-19 Temalı Siber Saldırı Haritası

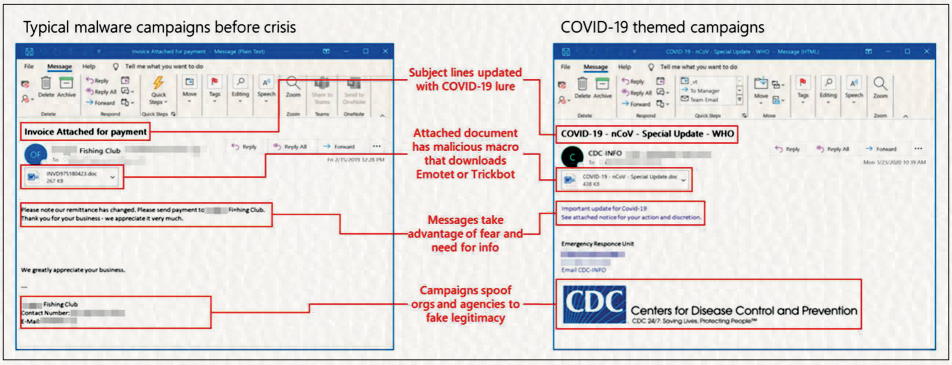
11.4.1. Sahte Alan Adları ve Web Sayfaları



Şekil 11.5. COVID-19 Tedavisinde Kullanıldığı İddia Edilen hydroxy-chloroquine Maddesi ile İlgili Yapılmış Sahte Bir Web Sayfasının Ekran Görüntüsü

ABD Başkanı Donald Trump'ın 19 Mart'taki bir brifingde COVID-19 tedavisinde kullanılabilecek bazı ilaç isimlerini (hydroxy-chloroquine, Plaquenil, azithromycin vb.) telaffuz etmesinin [5] hemen akabinde bu ilaç adlarını içeren sahte alan adları ve bu alan adları kullanılarak oluşturulmuş sahte web siteleri sayısında inanılmaz bir artış olmuştur [6]. Her ne kadar bu sahte web sayfaları Ulusal Siber Olaylara Müdahale Merkezleri (USOM) tarafından tespit edildikleri anda erişimleri engellense de, benzer başka alan adları da alarak saldırganlar faaliyetlerini sürdürmeye devam etmeye çalışmaktadır.

11.4.2.Oltalama Saldırıları



Şekil 11.6. COVID-19 ile İlgili Gönderilmiş Bir Oltalama Saldırısı Ekran Görüntüsü

Dünya COVID-19 salgını için büyük bir mücadele verirken ve bu salgın için henüz herhangi bir tedavi tam manada geliştirilememişken, bilgisayar korsanları bir krizi fırsata dönüştürebilmek için bu zor zamanlarda insanlara bir umut sunar gibi hastalığa çözüm bulduklarını iddia ettikleri epostaları göndererek zararlı yazılımları kurbanlarının bilgisayarlarına bulaştırmaya çalışmaktadırlar.

11.4.3. Uç-Nokta Saldırıları

Uç-noktalar bir organizasyonun verilerine, kimlik bilgilerine ve ortamına erişim noktasıdır. Pandemi dolayısıyla uzaktan çalışmaya bağlı olarak uzaktan erişim için uç noktalar artmış, dolayısı ile siber suçlular için hedeflenen yüzey alanları da artmıştır. Uç nokta güvenliği oldukça kritik bir konudur, zira veri ihlallerinin ve kötücül yazılım bulaşmasının çoğu son kullanıcı cihazlarında gerçekleşmektedir.

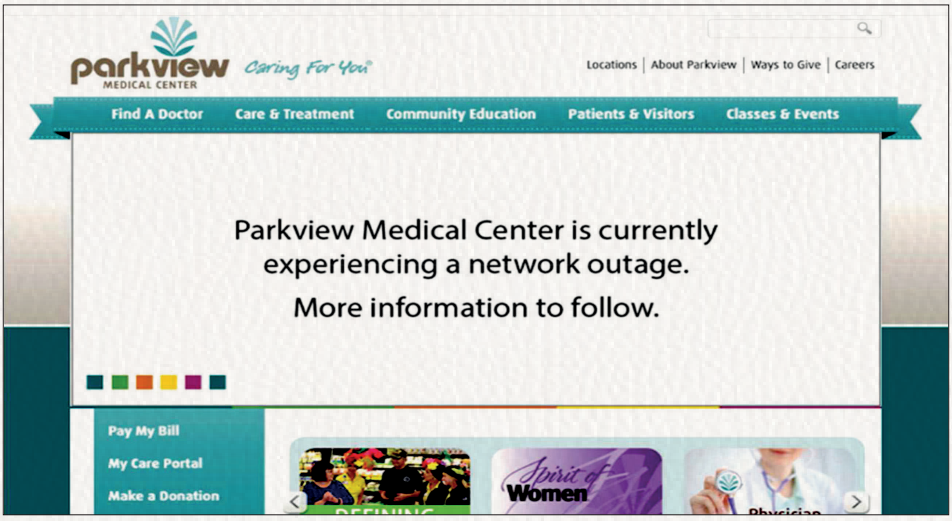
11.4.4. Uzaktan Eğitim Sistemlerine Saldırılar

Pandemi sürecinde birçok okul ve eğitim merkezi de uzaktan öğrenme sistemine geçip bu konu ile ilgili teknolojik altyapıları kullanmaya başlamışlardır. Bu sistemler de siber korsanların artan orandaki saldırılarına maruz kalmış ve eğitim seansları kayıtlarını içeren birçok veri internette paylaşılmaya başlan-

mıştır [7]. Videoların çoğu, katılımcıların seslerini, yüzlerini ve iletişim numaralarını ve başka kişisel verileri içermektedir. Ayrıca eğitimle ilgili notların da çevrimiçi tutulmak durumunda olduğu bu dönemde bazı siber korsanlar belli bir ücret mukabilinde sistemlere sızarak ders notlarını yükseltme hizmeti sunmaya başlamıştır.

11.4.5. Sağlık Bakanlıkları, Araştırma Laboratuvarları ve Hastanelere DDoS ve Fidye Yazılım Saldırıları

Tüm dünya genelinde güvenlik birimleri sağlık bakanlıkları, araştırma laboratuvarları ve hastanelere gerçekleştirilen siber saldırıların önemli ölçüde artış sağladığına dikkat çekerek, bilgisayar korsanlarının ulusal ve uluslararası sağlık politikası konusunda istihbarat elde etmeye veya COVID-19 ile ilgili araştırmalar hakkında hassas verileri ele geçirmeye çalıştıklarını söyleyerek ilgili tıbbi kurum ve kuruluşları uyarmışlardır [8]. Bazı saldırganlar ise sağlık çalışanlarının insan hayatını kurtarabilmek için saniyelerle yarıştığı böyle bir ortamda finansal gelir elde edebilmek için ya bu tıbbi kurum ve kuruluşların web sayfalarına DDoS saldırısı yaparak erişimi engellemiş ya da ransomware saldırıları ile hassas hasta/hastane verilerini şifreleyerek bu verilere tekrar erişim için para talep etmişlerdir.



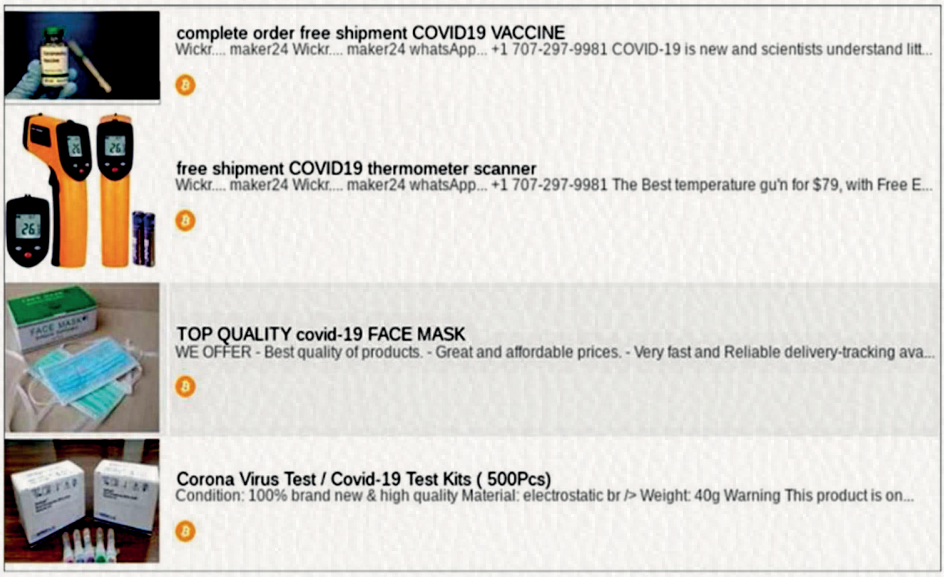
Şekil 11.7. Bir Hastaneye Yapılmış DDoS Saldırısı ile İlgili Ekran Görüntüsü

COVID-19 salgınının başlangıcından bu yana, DSÖ (Dünya Sağlık Örgütü), personeline yönelik siber saldırıların sayısında ve e-posta dolandırıcılıklarında çarpıcı bir artış görmüştür. DSÖ ağlarına gerçekleştirilen siber saldırıların geçen yılın aynı dönemine kıyasla beş kat artış gösterdiğini bildirmiştir. Salgının daha ilk ayında, yaklaşık 450 aktif DSÖ e-posta adresi ve şifresi çevrimiçi olarak sızdırıldı. Saldırının, mevcut ve emekli personel ile DSÖ paydaşlarının kullandığı eski bir extranet sisteminden kaynaklandığı belirtildi.

Bunun dışında Çek Cumhuriyeti'ndeki hastaneler sistemlerine yapılan siber saldırıları engellediği duyururken, İtalya'nın sosyal güvenlik sitesine erişim bir süreliğine engellendi.

11.4.6.DarkWeb'de Sahte Kit, Sahte İlaç ve Plazma Satışları

Siber güvenlik araştırmacıları, DarkWeb'de sahte COVID-19 aşıları, tanı kitleri ve daha önce hastalığı atlatmış kişilerden alındığı öne sürülen plazmaların satışa sunulduğu birkaç sanal pazar yeri keşfettiler [9]. Ayrıca bu pazarlarda satıcıların bunların yanı sıra listelerini yüz maskeleri, el dezenfektanı ve daha sonra chloroquine satışlarını içerecek şekilde çeşitlendirdiği gözlemlenmiştir.

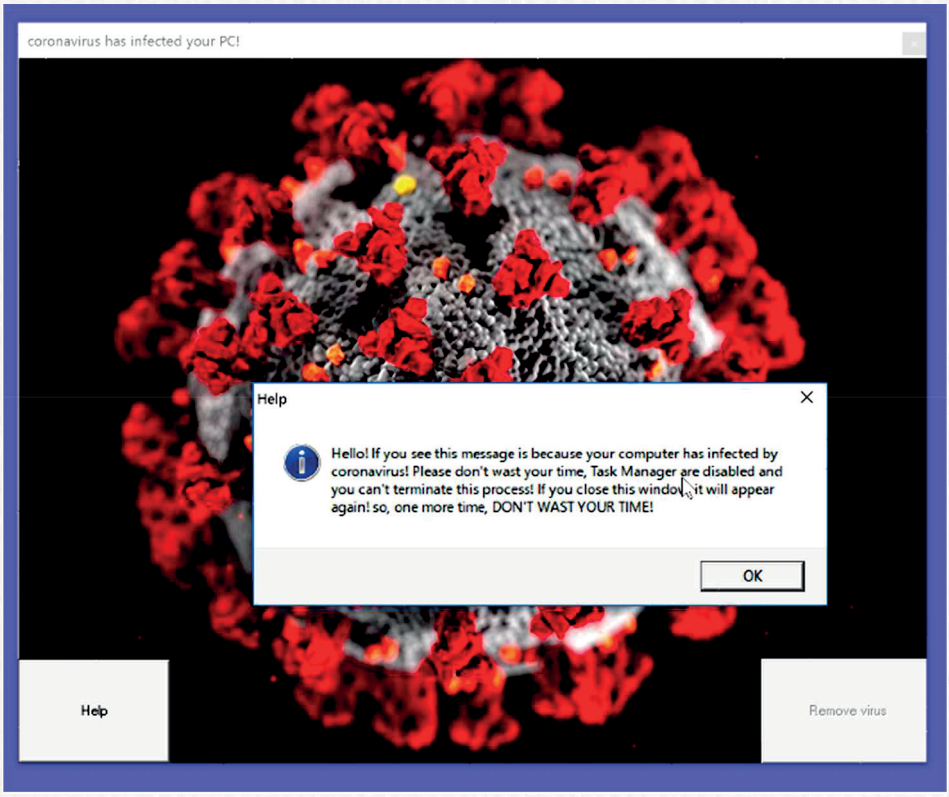


Şekil 11.8. DarkWeb'de Satışı Yapılan COVID-19 Tanı Kitleri ve İlaçlar ile İlgili Ekran Görüntüsü

11.4.7. Telekonferans Uygulamalarına Yapılan Saldırılar

Son zamanlarda, binlerce çevrimiçi toplantı kaydının hiçbir koruma olmadan internette erişime açık olduğu tespit edilmiştir [10]. Bu kayıtlarda birçok hassas bilgi paylaşıldığı ve bu bilgilerin siber korsanlarca kullanıldığı da bilinmektedir. Ayrıca bu telekonferans uygulamalarına yapılan ve kullanıcı bilgilerinin (kullanıcı adı ve şifre) ele geçirildiği saldırılar sonrası bu bilgiler hem internet üzerinden satışa çıkarılmış hem de bu bilgiler kullanılarak bilgileri çalınan kişinin başka hesaplarına da saldırılar düzenlenmiştir.

11.4.8. COVID-19 Kötücül Yazılımı



Şekil 11.9. Bir Bilgisayara Bulaşmış COVID-19 Kötücül Yazılımı Ekran Görüntüsü

Siber güvenlik uzmanları yakın bir zamanda, bir sistemin ana önyükleme kaydını (MBR) geçersiz kılan ve ön yüklenemez hâle getiren bir korona virüs temalı kötü amaçlı yazılımı analiz etmişlerdir [11]. Bu kötücül amaçlı yazılım çalıştırıldığında, makineyi otomatik olarak yeniden başlatır ve ardından kapatılamayan virüs temalı bir pencere görüntüler. Pencerenin sağ üst tarafındaki normal çıkış düğmesi ise çalışmamaktadır.

11.4.9. VPN Saldırıları

Mevcut VPN şifreleme protokolleri sağlam olabilir ve önemli koruma sağlar. Ancak hiçbir şey saldırıya karşı yüzde yüz bağışık değildir. Geleneksel olarak, VPN'lerde kullanılan Internet Anahtar Değişimi (IKE) [12], saldırganların hedefleri arasındadır.

Çoğu VPN servis sağlayıcısı, müşterileri için kullanıcı adları ve şifreler gibi önemli bilgileri içeren güvenlik riskleri oluşturabilecek kimlik doğrulama verilerini depolamayı önerir. Bu durum bilgi güvenliği açısından oldukça kritik ve istenmeyen bir durumdur. Ayrıca, hata mesajları ve paket başlıkları, çalışmakta olan VPN'nin türü ve sürümü hakkında saldırganlara oldukça önemli bilgiler verebilmektedir.

11.5. SALDIRILARA KARŞI TEDBİRLER

Devletler, pandemi sürecindeki siber tehditleri azaltmak için daha proaktif bir yaklaşım benimsemeye başladılar. Avustralya Sinyaller Müdürlüğü koronavirüs ile ilgili saldırıları ve kötü niyetli faaliyetleri engellemek için karşı saldırı (counter attack) siber yeteneklerini seferber ettiğini açıkladı. Amerikan Senatosu ABD Siber Savunma Komutanlığı'na sağlık sektöründeki siber tehdit eylemlerini tespit etme, değerlendirme ve caydırma hususunda tam yetki verdi. Yine ABD Adalet Bakanlığı yüzlerce kötücül amaçlı COVID-19 web sitesini kaldırmak için teknoloji şirketleri ile iş birliğini arttırmıştır.

Önde gelen teknoloji şirketleri tarafından birkaç girişim daha başlatıldı. WhatsApp ve Facebook, kendi platformlarında yanlış bilgilerin yayılmasını sınırlamak için adımlar attı. Facebook, 50'den fazla dilde yapılan paylaşımların bilgi kontrol ve içerik derecelendirmesi için dış denetçiler görevlendirmek adına bağımsız bir kuruluşla iş birliği yaptığını duyurmuştur.

11.5.1. Kullanıcılara Yönelik Sorumluluklar

Herhangi bir siber güvenlik zincirinde en güçlü ve en zayıf halka insanlardır. Bir kurum ya da kuruluş aktif ağ taraması ile en gelişmiş tehdit istihbarat programına sahip olsa dahi zararlı bir yazılımı önce kendi bilgisayarına daha sonra organizasyon ağına bulaştıracak bir bağlantıyı tıklatmak yalnızca bir çalışanı gerektirir. Kuruluş ne kadar güvenli olursa olsun, ne kadar karmaşık çözüm ve politikalar uygulanmış olursa olsun personel belirlenen yönetim süreçleri altında faaliyet göstermiyorsa, derinlemesine savunma güvenlik katmanları kuruluşun korunmasında daha az etkili hâle gelmiştir. Dolayısı BT departmanlarının aldığı güvenlik tedbirlerinin ötesinde bireysel kullanıcılara da oldukça önemli sorumluluklar düşmekte ve gerek kendi kişisel verilerini gerekse parçası oldukları organizasyona ait hassas verileri korumakla yükümlüdürler.

11.5.2. Organizasyonlara Yönelik Sorumluluklar

İster büyük ister küçük bir organizasyonda, güçlü politikalar belirlemek, mevcut kontrolleri geliştirmek ve son kullanıcılara eğitimler sunmak, durumsal farkındalığı arttırmaya yardımcı olacak en iyi uygulamalardır. Hassas işler yapan kuruluşlar, faaliyetlerinin doğası gereği her zaman siber saldırganlar için bir hedeftir. Örneğin, çevrimiçi bankacılık, bir şirketin finansal suçlar için tanımlanması ve hedeflenmesi riskini arttırır. Büyük holdingler ya da Fortune 500 şirketleri, tehdit yüzeyini genişleten bir markaya sahiptir. Bahsi geçen organizasyonlar bu çok çeşitli siber olayları tanımlayabilmeleri ve bu saldırılara hazırlıklı olarak yanıt verebilmelidirler.

11.5.3. Siber Operasyon ve Siber Olaylara Müdahale Merkezleri

Önce cephede savaş veren SOM analistleri, güvenlik tehditlerini analiz etmek ve bunlara müdahale etmekten sorumludur. Kurumsal ofislerde çalışmaktan evden/uzaktan çalışmaya geçilen dolayısı ile uzaktan erişim ve uzaktan bağlantı gerektiren bu yeni dönemde SOM analistlerinin günlük karşılaştığı rutin network trafiği ve bu trafiğe yönelen tehditler de değişmiştir. Böyle kaotik bir durum göz önüne alındığında, saldırganlar inanılmaz derecede kısa bir sürede çeşitli teknikler, taktikler ve prosedürlerle seferber olabilmektedir. SOM analistleri açık kaynak siber tehdit istihbaratı (OSINT) ile saldırılar gerçekleşmeden önce olası siber saldırı analizleri yaparak bu doğrultuda adım atmaktadırlar.

Ulusal çapta ise Siber Olaylara Müdahale Merkezleri (USOM'lar) network trafik analizi gerçekleştirmekte, önemli kaynaklardan siber tehdit istihbaratı toplayarak Ulusal Bilişim Güvenliğine tehdit gördükleri hususlarla ilgili önemli çalışmalar ile gerçekleştirilen ya da gerçekleştirilmesi muhtemel siber saldırıların engellenmesi ya da en az zararla önüne geçilmesi adına faaliyetlerini sürdürmektedir.

11.6. ULUSAL BİLİŞİM GÜVENLİĞİ

Ülkemizin 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı [13] incelendiğinde siber güvenliğin ulusal güvenliğimizin bir parçası olduğu görülmektedir.

COVID-19 sonrası bu yeni dönemde kriz süresince gözlemlenen siber aktör ve tehditler göz önüne alınarak Ulusal bilişim güvenliğini yeni bir bakış açısı ile ele almamız önemli ve kritik bir adım olacaktır. Bu yeni dönemde olabilecek risk ve tehditleri şu şekilde sıralayabiliriz:

- Küresel salgın sonrası IoT temelli akıllı şehirler, blokzincir teknolojisine dayanan dijital vatandaşlık servisleri, yapay zekâ ve büyük veri üzerine kurulu hizmetlerin artması ve bu hizmetlerin güvenliğine yönelik yaklaşımların önem kazanması.
- Uzaktan çalışma modelinin, siber tehdit yüzeylerini arttırarak kurumların yoğun bir şekilde siber saldırılara maruz kalmasına neden olması.
- Hâlihazırda güvenlik nedeniyle internete açık olmayan kapalı ve gizlilik dereceli ağların, uzaktan çalışma gerekliliği kapsamında yeterli risk değerlendirmesi yapılmadan internete kontrolsüz olarak açılarak veri sızıntısına neden olması.
- Dışa bağımlı bilişim teknolojileri yatırımlarında tedarik zincirlerinden ve 3. taraflardan kaynaklanan sorunlar yüzünden, siber saldırılara karşı kritik altyapıların dayanıklılığının ve sürekliliğinin sağlanmasının zorlaşması.
- Vatandaşların e-devlet uygulamalarındaki kullanım artışı, kişisel bilgisayarların güvenliğinin de önem kazanmasına neden olması.
- Ülkemizce geliştirilen ve verilen ülkemizde tutulduğu bulut altyapılarının azlığı ile ulusal bilgi güvenliği farkındalığının eksikliğinden

kaynaklı nüfus, sağlık ve iletişim bilgileri gibi kritik verilerin kontrolsüz olarak yurt dışı kaynaklı bulut servislerinde işlenme ihtimalinin artması.

- COVID-19 ile mücadele sürecinde de görüldüğü önemli sosyoekonomik olaylar sırasında, sosyal medya ve internet aracılığı ile kasıtlı olarak oluşturulan yanlış haber ve bilgi kirliliğinin kamu düzenini olumsuz olarak etkilemesi.
- Siber olaylara karşı, kurumlar arası koordinasyon eksikliğinden kaynaklı hızlı ve etkin müdahalenin yapılamaması.
- Her türlü kurum ve kuruluşta oltama postaları, zararlı yazılım ve benzeri saldırılar sonucunda dolandırıcılıkla yoğun bir şekilde karşı karşıya kalınması.
- Hastalığın gidişatı ilgili daha fazla veri toplamak için kullanılan mobil uygulamaların kişisel verileri ifşa ettiği ve gizlilik kaygılarının ön plana çıkmasına neden olması [14].
- BT altyapı ve hizmetlerinde kritik rolde olan personelin küresel salgın nedeniyle seyahat edememesi veya hasta olması gibi durumunda alternatif önlemlerin belli olmaması.
- Uzaktan çalışma modelinde mobil cihazların ve iletişim kanallarının şifreli olmaması veya şifrelemenin millî kripto çözümleri ile sağlanmaması.
- Video/telekonferans iletişiminin küresel BT firmaların bulut çözümleri ile yapılmasının ulusal bilgi güvenliği zafiyetine yol açması.
- Uzaktan çalışma esaslarına yönelik yasal mevzuat boşluğunun, bilgi güvenliği süreçlerini etkin ve doğru olarak yönetmeyi zorlaştırması.
- Ofisten ve uzaktan çalışma modellerinin kullanıldığı dağıtık BT mimari yapısına sahip kurumlarda siber güvenliğe yönelik izlenebilirlik ve olay müdahale süreçlerinin zorlaşması.
- Siber risk yüzeyinin artması ile IoT, yapay zekâ, kritik altyapılar, bulut, büyük veri ve yapay zekâ teknolojileri gibi alanlarda siber savunma ve saldırı yöntemlerinin tam olarak bilinmemesi ve bu siber güvenlik yaklaşımlarında yetkin ve nitelikli personel eksikliğinin ortaya çıkması.

- Pandemi sonrası uzaktan çalışma nedeniyle BT hizmetlerindeki artan kapasite ihtiyaçlarına hızlı cevap vermek adına plansız ve kontrolsüz olarak sağlanan servisler ile güvenlik gereksinimlerinden taviz verilmeye başlanması.

Ulusal bilgi güvenliği, ulusal kalkınma hedefleri ile doğrudan ilintili olup ekonomik ve sosyal fayda üreten bilgi sistemleri ile kritik altyapıları korumak adına ayrı bir önem arz etmektedir. Bu noktada ulusal bilgi güvenliği stratejileri belirlenirken hem kamu hem de özel sektörün eşgüdüm içerisinde çalışacakları kurumsal bir yapı hazırlanmalıdır. Küresel salgın sonrası, ulusal bilgi güvenliğine dair yol haritasında şu noktalar daha bir önem kazanacaktır:

- Özellikle Blokzincir ve Yapay Zekâ teknolojilerinin siber savunmada kullanımı için gerekli araştırma ve geliştirmelere bütçeleri ayrılarak bu konuda nitelikli iş gücü ve millî ürünlerin arttırılması teşvik edilmelidir.
- Ulusal Siber Olaylara Müdahale Merkezinden ayrı kritik alt yapılar için spesifik faaliyet gösteren bir Ulusal Siber Olaylara Müdahale Merkezi kurulmalıdır.
- Bilgi paylaşımı ve kolektif savunmada önemli roller üstlenen Bilgi Paylaşım ve Analiz Merkezleri (Information Sharing and Analyzing Center – ISAC) sektör bazlı kurulmalı ve desteklenmelidir.
- Hızlı değişen dijital dönüşüm talepleri nedeniyle Ulusal Siber Güvenlik Stratejisi ve Eylem Planlarının 3 yılda bir yerine, yıllık olarak güncellenmesi gerekmektedir.
- Uç nokta güvenliği, ağ güvenliği ve iletişim güvenliği için kamu ve özel kurumlar, Millî Açık Anahtar Altyapısı (MA3) [15] gibi tamamıyla yerli ve millî kriptografik çözümler kullanmalıdır.
- Kurumlara ait gizlilik dereceli haberleşmenin yerli ve millî kripto sistemleri ile geliştirilen güvenli ağ cihazları (AGC) [16] üzerinden gerçekleştirilmesi sağlanmalıdır.
- Güvenli kamu internet ağının (KAMUNET) yaygınlaştırılması sağlanmalıdır.
- Yurt içinde oluşturulan nüfus, sağlık, iletişim gibi kritik verilerin yerli bulut teknolojileri ile ülkemiz sınırları içerisinde yer alan sunucularda güvenli olarak saklanmalı ve bu tür çözümlerin yaygınlaştırılmalıdır .

- Siber güvenlik çözümlerinde makine öğrenmesi ve derin öğrenmeye dayalı tehdit algılama, saldırı önleme ve davranışsal analiz yaklaşımları kullanılarak otomatik yanıt veren Güvenlik Düzenleme, Otomasyon ve Yanıt (Security Orchestration, Automation, and Response – SOAR) sistemler kullanılmalıdır. Bu kapsamda siber tehdit analizinde kullanılmak üzere ulusal veri setleri hazırlanmalıdır.
- Bilgi güvenliğine yönelik ulusal risklerin belirlenip merkezî olarak risk yönetiminin tek bir otorite tarafından yürütülmesi sağlanmalıdır.
- Ulusal bilgi güvenliği alanlarında Ar-Ge faaliyetlerinin desteklenmesi için üniversitelerle iş birliği yapılarak bilgi güvenliği yüksek lisans ve doktora programlarının sayısının nitelik ve nicelik olarak arttırılması sağlanmalıdır.
- Başta enerji, finans ve iletişim sektörleri olmak üzere Türkiye'nin kritik altyapılarına yatırım yapan şirketlerin yabancı ortaklı özel girişimler olduğu düşünüldüğünde bu girişimlerin uyması gereken zorunlu siber güvenlik tedbirleri sıkıca denetlenmelidir.
- Gelişen teknoloji ile eş zamanlı olarak siber güvenlik ihtiyaçlarını karşılayacak hukuki düzenlemelerin hızlıca hayata geçirilmesi gerekmektedir. Yasal düzenlemelerin, bilişim alanındaki uluslararası hukuki düzenlemeler ile uyum içinde olması sağlanmalıdır.
- Kurumsal bilgi güvenliği yönetişim süreçleri, kamu kurumlarında zorunlu hâle getirilmelidir.
- Global pazarda rekabet edebilmek için yerli ve millî siber güvenlik ürünlerinin test ve sertifikasyonuna yönelik, uzman personel ve laboratuvar sayılarının arttırılmalıdır.
- Siber güvenlik alanında başta kamu kurum ve kuruluşları ile özel sektör girişimleri ve tüm bireylerin ihtiyaçlarını pratikte karşılayacak güvenlik yapılandırma kılavuzlarının, sistemlere yönelik sıkılaştırma rehberlerinin ve en iyi uygulama tecrübelerinin belirtildiği dokümanların ele alındığı bir portal hazırlanarak güncelliği sağlanmalı ve bu dokümanlar herkese açık çevrim içi ortamda yayınlamalıdır.

11.7. SONUÇ VE DEĞERLENDİRMELER

Küresel salgınla mücadelede ön plana çıkan sosyal mesafe kavramı ile çalışma şartları yeni bir boyut kazanmış, mekân bağımlılığı ortadan kalkarak uzaktan veya evden çalışma modeli daha da bir önem kazanmıştır. Bilişim teknolojilerinin hayatın her alanında kullanılması yeni bir dijital yaşam kültürünü de ortaya çıkarmıştır. Pandemi adeta hızlı bir şekilde dijital dönüşümü de zorunlu hâle getirmiştir. Bu dijital dönüşüm de, siber uzayın taşıdığı tehdit ve riskleri de beraberinde getirmektedir.

Avrupa Birliği ve Dünya Sağlık Örgütü gibi uluslar üstü örgütlerin küresel salgındaki yetersiz ve güçsüz kalmaları, kendi mücadelesini tek başına veren güçlü devlet kavramını ön plana çıkarmıştır. Bu bağlamda, bilişim güvenliği de kritik altyapıların dayanıklılığının ve sürekliliğinin sağlanması açısından ulusal güvenliğin önemli bir boyutu olarak ele alınmalı, "yeni normal dönem"de ulusal siber güvenlik ekosisteminin yaygınlaştırarak yerli ve millî çözümleri üreten ve etkin kullanan bir anlayış egemen kılınmalıdır.

Bu süreçte gerçekleştirilen siber uzaydaki faaliyetler analiz edildiğinde şu değerlendirmelere mümkün olacaktır;

- Siber suçlular, taktik ve planlarını kurbanlarını cezbetme olasılığı daha yüksek olan yerel olaylardan faydalanmak için uyarlar. Temeldeki kötücül amaçlı yazılım tehditleri devam ederken saldırı yöntem ve stratejileri hızlı ve akıcı bir şekilde değişmektedir.
- Siber savunma yatırımlarında en iyi etki alanları arası sinyal analizi, güncelleme yönetimi ve kullanıcı eğitimi gösterilebilir. Saldırı maliyetini arttıran veya başarı olasılığını azaltan yatırımlar en uygun savunma stratejileri arasındadır.
- Siber saldırganların taktik ve tekniklerini analiz etme, siber tehdit istihbaratını da kullanarak saldırılardan daha gerçekleşmeden haberdar olma, derin ve çoklu katmanlı savunma stratejileri benimseme ülkelerin ve organizasyonların siber güvenlik politikaları açısından önem arz etmektedir.

KAYNAKLAR

[1] Samonas, S. ve D. Coss. 2014. "The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security." *Journal of Information System Security* 10(3): 21–45.

[2] "Microsoft shares new threat intelligence, security guidance during global crisis," Microsoft Security, Apr. 08, 2020. https://www.microsoft.com/security/blog/2020/04/08/microsoft-shares-new-threat-intelligence-security-guidance-during-global-crisis/ (accessed Jun. 22, 2020).

[3] "Exploiting a crisis: How cybercriminals behaved during the outbreak," Microsoft Security, Jun. 16, 2020. https://www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-during-the-outbreak/ (accessed Jun. 22, 2020).

[4] "Threat Landscape Mapping Infographic 2020." https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/threat-landscape-mapping-infographic-2020 (accessed Jun. 22, 2020).

[5] Reuters. 2020. "Special Report: Doctors Embrace Drug Touted by Trump for COVID-19, without Hard Evidence It Works."

[6] SentinelLabs. "Threat Intel | Cyber Attacks Leveraging the COVID-19/CoronaVirus Pandemic." Retrieved May 14, 2020 (https://labs.sentinelone.com/threat-intel-update-cyber-attacks-leveraging-the-covid-19-coronavirus-pandemic/).

[7] Cosn. "COVID-19 & Cybersecurity - Member Exclusive.Pdf." Retrieved May 14, 2020 (https://www.cosn.org/sites/default/files/COVID-19%20%26%20Cybersecurity%20-%20Member%20Exclusive.pdf).

[8] Healthcare IT News. "Cyber-Attacks on Healthcare Facilities 'growing Threat' during Coronavirus Pandemic." Retrieved May 14, 2020 (https://www.healthcareitnews.com/news/europe/cyber-attacks-healthcare-facilities-growing-threat-during-coronavirus-pandemic).

[9] Majumdar, Romita. 2020. "Coronavirus: Fake COVID-19 Drugs, Vaccines Thrive on Dark Web." *Livemint*. Retrieved May 14, 2020 (https://www.livemint.com/news/india/dark-web-criminals-peddle-fake-covid-19-vaccines-as-a-front-for-malware-attacks-11587390740238.html).

[10] Norton. "Video Conferencing Risks When Working at Home: 16 Ways to Avoid Them." Retrieved May 14, 2020 (https://us.norton.com/internetsecurity-emerging-threats-zoom-bombing-video-conference-threats.html).

[11] Trend Micro. "Developing Story: COVID-19 Used in Malicious Campaigns - Новости о Безопасности - Trend Micro TR." Retrieved May 14, 2020 (https://www.trendmicro.com/vinfo/tr/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains).

[12] Threat Post. "Government VPN Servers Targeted in Zero-Day Attack." Retrieved May 14, 2020 (https://threatpost.com/government-vpn-servers-zero-day-attack/154472/).

[13] T.C. Ulaştırma ve Altyapı Bakanlığı. n.d. Retrieved May 27, 2020 (https://www.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf).

[14] Romm, Tony, "U.S. Government, Tech Industry Discussing Ways to Use Smartphone Location Data to Combat Coronavirus." *Washington Post*. Retrieved May 27, 2020 (https://www.washingtonpost.com/technology/2020/03/17/white-house-location-data-coronavirus/).

[15] TUBİTAK BİLGEM, "Millî Açık Anahtar Altyapısı.| MA3." *BİLİŞİM ve BİLGİ GÜVENLİĞİ İLERİ TEKNOLOJİLER ARAŞTIRMA MERKEZİ*. Retrieved May 27, 2020. (https://ma3.bilgem.tubitak.gov.tr/).

[16] TUBITAK BILGEM. "AGC-G - Gigabit Ağ Güvenlik Cihazı." *BİLİŞİM ve BİLGİ GÜVENLİĞİ İLERİ TEKNOLOJİLER ARAŞTIRMA MERKEZİ*. Retrieved May 27, 2020 (https://bilgem.tubitak.gov.tr/tr/icerik/agc-g-gigabit-ag-guvenlik-cihazi).

[17] GMS - Güvenli Mesajlaşma Sistemi | BİLİŞİM ve BİLGİ GÜVENLİĞİ İLERİ TEKNOLOJİLER ARAŞTIRMA MERKEZİ." https://bilgem.tubitak.gov.tr/tr/icerik/gms-guvenli-mesajlasma-sistemi.

Bölüm 12

DevSecOps

Murat Kaya - Tuğkan Tuğlular

Bu bölümde DevOps ve DevSecOps kavramlarına değinilmiş olup, DevOps'tan farklı olarak genel bir DevSecOps sürecinde yer alan aşamalar, kullanılabilecek yöntemler, araçlar ve kaynaklar irdelenmiştir. DevSecOps giderek önem kazanmaktadır ve yazılım firmaları tarafından yoğunlukla kullanılmaya başlanmıştır. Ancak üzerinde yapılan akademik çalışmaların ve kaynak yayınların azlığı nedeni ile literatür açısından hâlen zayıf bir alandır. Bu bölümde sunulan bilgiler ağırlıklı olarak web kaynaklarından derlenmiştir.

12.1. GİRİŞ

Uygulama güvenliği kavramları geçmişte geliştiriciler için bir odak noktası olmaktan uzak, çoğu zaman üretim zincirinin en sonunda yer almış veya göz ardı edilmiştir. Bunun nedeni, klasik uygulama geliştiriminde önemli olan ürünün bir an önce hizmete sunulması ve bu üretim sürecini engelleyecek her türlü yaklaşımdan uzak durulmasıdır. Bu nedenle güvenlik kavramı yıllarca, özellikle yazılım geliştirme sektöründe, engelleyici bir faktör olarak düşünülmüştür.

Aradan geçen zamanda, teknolojinin de gelişmesi ile birlikte, artık bilgi daha kolay ulaşılabilir ve paylaşılabilir olmuş, bunun yanı sıra bilgiye yönelik risk-

ler de aynı oranda artış göstermiştir. Bu süreç içerisinde yazılım ürününün hızlıca geliştirilmesi ve üretilmesi kadar, ürünün ve sunduğu bilginin değeri ve buna bağlı olarak güvenliği/güvenirliği de önem kazanmıştır.

Günümüzde uygulamaların güvenliğinin son derece önemli olduğu artık kabul edilen bir gerçektir. Önceleri, sadece bilişimde benzer meslek grupları arasında tartışılan siber güvenlik ihlalleri ve sorunları, artık neredeyse, tüm sosyal medya ve haber servislerinde ilk sıralarda yer almakta, hemen hemen her gün bir şirketin veya kurumun bilgilerinin ele geçirildiğine ve internet üzerinde yayınlandığına dair haberler çıkmaktadır.

Gittikçe artan bu siber saldırılar ve kötü sonuçları neticesinde, önceleri sadece fiziksel ve sistem seviyesinde dikkate alınan güvenlik önemlerinin artık sistemlerde çalışan yazılımlar ve uygulamalar için de ele alınması gerekliliği doğmuştur. Yazılımlar ve uygulamalar, doğası gereği (genellikle donanımlar ve altyapılar kadar sabit ve kararlı olmadığından) siber güvenlik saldırılarından ve ihlallerden en çok etkilenen yapılar olmuşlardır.

Bu noktada güvenli yazılım geliştirimi ve sürekli iyileştirme konuları öne çıkmış ve şu soru gündeme oturmuştur; güvenli ve güvenilir bir yazılım/uygulama geliştirme stratejisi planlarken üzerinde düşünülmesi gereken hususlar nelerdir? İlk akla gelen genellikle, bilginin veya verinin, erişim hakkı bulunmayan kişilere karşı korunması olabilir. Ancak daha önemlisi, veri veya bilgilerin, izinsiz bir şekilde değiştirilmediğinden veya silinmediğinden ya da standartlar ve prosedürler çerçevesinde yok edildiğinden ve geri döndürülemez olduğundan da emin olmamız gerekir.

Tüm bunların yanında, verilere kimlerin eriştiğini doğru bir şekilde doğruladığımızdan ve doğru izinlere sahip olduklarından emin olmamız, herhangi bir zamanda yaşanacak bir ihlal veya hata sonucunda arşiv verileri veya günlükleri aracılığıyla olayın sebebi ve oluşu ile ilgili kanıtlar bulabilmemiz gerekir.

Güvenlik, bilinenin aksine, bir uygulamaya veya sisteme daha sonra veya son aşamada ekleyebileceğiniz bir şey değildir. Güvenli geliştirme, yazılım geliştirme yaşam döngüsünün her aşamasının bir parçası olmalıdır. Bu yaklaşım, kritik uygulamalar ile hassas veya çok gizli bilgileri işleyen uygulamalar için daha da fazla önem teşkil etmektedir.

Yukarıda bahsettiğimiz gibi uygulama ve yazılım kaynaklı hataların, güvenlik açıklarının makul bir seviyede önlenebilmesi için baştan sona güvenliği düşü-

nülerek tasarlanmış ve bir süreç içerisinde devamlılığı sağlanmış uluslararası kabul görmüş ve geçerliliği kanıtlanmış metotlar kullanılması gereklidir. Bu tür metodolojilere veya sistemlere genel olarak "Güvenli Yazılım Geliştirim Döngüsü" denilmektedir.

Tüm bu süreçlerin, yazılım güvenliği ile ilgili olsun olmasın, yönetilmesinde birçok yöntem olsa da genel olarak insan gücü ile işletilmeye çalışılması hem zaman hem de maliyet açısından ciddi önem teşkil etmektedir. Hemen hemen her gün, hatta gün içerisinde birden çok defa hazır hâle getirilmesi ve uygulanması zorunlu olan iş süreçlerinin ve sistemlerin, el ile yönetilmesi hem hatalara hem de ciddi zaman kaybına yol açabilmektedir. Bu sebeple yazılım geliştirme süreçlerinde ortaya çıkabilecek hata ve sorunları en aza indirmek, zamandan kazanmak ve daha kolay devreye alım, yayınlama gibi faydalar sağlamak amacı ile DevOps/DevSecOps olarak adlandırılan ve bahsi geçen süreçleri otomatikleştirmeyi sağlayan yapılar/yöntemler kullanılmaktadır.

Burada ana konumuz DevSecOps olmakla beraber, DevSecOps süreci aslında DevOps sürecinin güvenlik ve güvenilirlik bağlamında genişletilmesi sonucunda ortaya konduğundan DevOps konusuna öncelikle değinilmiştir.

12.2. DevOps

DevOps'un Genel Tanımı

Geliştirme (Development-Dev) ve Operasyon (Operations-Ops) süreçlerinin bir araya getirilmesi ve hatta bütünleşik çalıştırılması olan DevOps, müşterilere sürekli olarak değer sunmak için bir araya gelen ekiplerin, süreçlerin ve teknolojilerin bütünü olarak tanımlanabilir. DevOps, daha kaliteli yazılım ürünleri üretmek amacıyla koordinasyon ve iş birliği gerçekleştirmeyi hedefler. Özellikle klasik üretim anlayışında mevcut olan birbirinden ayrı düşünülen geliştirme, bilgi teknolojileri (BT) operasyonu, kalite mühendisliği ve güvenlik rollerinin ekip ve süreç içerisinde bir arada ve bütünleşik bulunmasına olanak tanır.

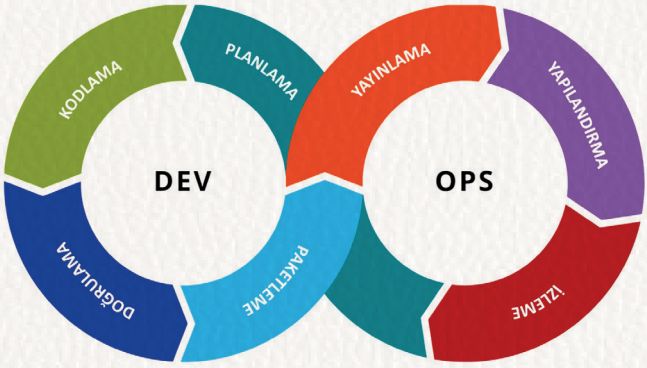
Geleneksel üretim mantığından farklı olarak ortaya çıkan bu kültür ve iş yapış biçimi, firmaların ve işletmelerin müşterilerine daha iyi, daha hızlı ve kaliteli hizmet sunmasına ve piyasada daha etkili bir şekilde rekabet etmesine imkân tanımaktadır.

DevOps'un Yazılım Yaşam Döngüsündeki Yeri

DevOps tüm yazılım yaşam döngüsü boyunca sürece dâhil olan bir süreçler sistemidir. Planlama, geliştirme, teslim ve çalıştırma aşamaları boyunca uygulama yaşam döngüsüne etki eder. DevOps kültüründe roller ve aşamalar birbiriyle ilişki içerisindedir. Tek bir rol tek bir süreç yaklaşımı yerine birbiri ile etkileşimli ve iç içe geçmiş rollerden ve süreçlerden bahsedilebilir.

DevOps Aşamalarına Genel Bakış

DevOps aşamaları Şekil 1'de gösterilmiştir. Bu bölümde anılan aşamalar kısaca açıklanmıştır.



Şekil 12.1. Genel DevOps Yaşam Döngüsü [2]

Planlama

Bu aşamada DevOps ekipleri geliştirilecek uygulama ile ilgili sistem, altyapı ve özellikleri tasarlar, bu tasarıma ilişkin çeşitli tanım ve açıklayıcı dokümanları oluştururlar. Aynı zamanda çeşitli DevOps yönetim araçları ile bu süreci baştan sona izlenebilir hâle getirirler. Bu araçlara örnek vermek gerekirse Scrum ile çevik yazılım süreçlerini yönetme, Kanban panoları ile süreci ve ilerlemeyi görselleştirme verilebilir. Bunlara ek olarak, pek çok DevOps izleme ve raporlama araçları ile süreç daha kolay ve sağlıklı yönetilebilir.

Geliştirim

Geliştirim ya da geliştirme aşaması, uygulama için yazılan kodların yine aynı ekip tarafından test edilmesi, gözden geçirilmesi ve bir araya getirilmesine ek olarak farklı ortamlarda derlenebilir ve çalıştırılabilir hâle getirilmesi sürecini içerir.

DevOps takımının nihai hedefi yeni bir özellik kazandırılmış uygulamanın kaliteden ödün verilmeksizin ve en hızlı şekilde müşteriye sunulması olduğundan burada hız ve kalite sağlayabilmek adına rutine bağlı ve insan müdahalesi ile gerçekleştirilen tüm işlemler otomatikleştirilir.

Yayınlama

Yayınlama ya da sürüm, geliştirimi tamamlanmış uygulamaların çeşitli ürün dağıtım ortamlarında hızlı, güvenli kanallar vasıtası ile müşteriye ulaştırılması veya yayınlanması sürecidir. Bu süreçte DevOps ekipleri tarafından bir takım kontrol ve onay süreci tasarlanır. Bu süreç, elle gerçekleştirilebildiği gibi otomatikleştirilerek daha sonrası için genişletilebilir, ölçeklenebilir veya tekrar tekrar kullanılabilir hâle getirilebilir. Bu tür bir yapının kurulması DevOps ekiplerinin ürünlerini tereddüt etmeden yayınlayabilmelerine olanak tanır.

İzleme ve Kontrol

İzleme ve kontrol aşaması, uygulamaların yayınlama sonrası her türlü bakım, izleme ve hata yönetimi gibi süreçlerini kapsamaktadır. Sistem güvenirliği ve yüksek erişilebilirlik hedeflenirken aynı zamanda güvenlik ve doğruluğu da en yüksek düzeyde tutmaya odaklanılır. Klasik yaklaşımda olduğu gibi hatanın müşteriden gelmesini beklemek yerine hatayı önceden tespit edebilecek çok çeşitli ölçüm ve izleme sistemleri kullanılır. Bu sayede müşteriye herhangi bir olumsuz durum yansıtmadan sorun giderilerek en iyi müşteri deneyimi sunulması hedeflenir. Buradaki diğer bir başarı kriteri ise tüm sistemlerin en yüksek derecede izlenebilirliğini sağlamaktır.

DevOps Kültürü

DevOps kültürü teknolojinin kullanılması ile süreçlerin otomatikleştirilmesi ve verimli hâle getirilmesi gibi görülse de aslında en önemli faktör her zaman olduğu gibi insanın kendisidir. Her şirketin veya kurumun kendine has bir iş yapma şekli ve kültürü bulunmaktadır. DevOps'un başarılı uygulanabilmesi bu kültürde bir takım radikal değişikliklere gidilmesi zorunluluğunu doğurabilir. Gerçek ve başarılı bir DevOps ancak iş yapma biçimlerinin DevOps kültürüne uyumu ve sürece olan yüksek bağlılık ile mümkün olabilmektedir.

Bu konudaki en büyük sorun genellikle klasik yazılım ve uygulama geliştirme kültürüne sahip ekiplerin ilk başta DevOps kültürüne karşı olan olumsuz

tutumları ve adaptasyon problemleri olmaktadır. Bu yüzden DevOps ekibi kurmadan önce bu konu mutlaka göz önünde bulundurulmalıdır.

Başarılı bir DevOps ortamında yazılım geliştirme ve bilgi teknolojileri gibi farklı alanlardaki ekipler tüm süreç boyunca birbirleri ile iletişim hâlinde olmalıdır. Sadece çalışma anlamında değil aynı zamanda planlama ve hedeflerin belirlenmesi aşamasında da birlikte ve bir uyum içerisinde hareket etmelidirler.

Ekiplerin birbirleri ile olan bu etkileşimi ve ortak yaşam döngüsü bir süre sonra rollerin sadece belli kişiler üzerinde yoğunlaşmasından çok ekip içerisinde farklı kişilere birden çok farklı roller şeklinde yansımaktadır. Özetle bir kişi tek bir iş ile meşgul olmak yerine birden fazla şapka takacaktır. Örneğin, geliştirme ekibi sadece kod yazmaktan sorumlu olmak yerine bir süre sonra yayınlama, kalite kontrol ve performans gibi konularda da sorumluluk alabilecektir.

DevOps'un en büyük getirilerinden biri kısa zaman aralıklarında sık ve güvenilir üretim yapılabilmesine olanak sağlamasıdır. Süreçler belirli kişiler üzerinde yoğunlaşmadığından ve otomatikleştirildiğinden hızlı biçimde sürümler çıkabilmektedir.

DevOps ekipleri, tıpkı bir yazılımın sürekli olarak ilerlemesi ve gelişmesi gibi kendisini de bu süreç içerisinde geliştirebilmektedir. İlk başlarda birçok hata yapılsa da zamanla bu hatalardan öğrenme ile daha istikrarlı ve kaliteli bir ekip ortaya çıkacaktır.

DevOps kültürünü ve yaklaşımını tam anlamıyla benimsemiş olan ekipler üretim gücü ve sürekliliğini ciddi derecede arttırabilmektedir. Buna bağlı olarak ürünlerin pazarlama süreleri kısalmakta, rekabet gücü artmakta, sistemin devamlılığı ve güvenirliği sağlanmakta ve hata yönetimi süreçleri iyileşmektedir.

DevOps Uygulamaları

Sürekli Entegrasyon

Sürekli entegrasyon (Continuous Integration-CI), yazılımı geliştiren ekibin üretmiş olduğu kodların belirlenen planlar çerçevesinde düzenli olarak merkezî bir depoda/arşivde toplanması, burada birleştirilerek otomatik olarak derlenmesi, test edilmesini içeren işlerin otomatikleştirildiği bir DevOps uygu-

lamasıdır. Sürekli entegrasyon sırasında birçok hata tespit edilebilir, önceden belirlenen sınır değerler ve kurallar doğrultusunda belirli bir kalite ölçüsünün altında kalındığı durumlar tespit edilerek derleme, test ve/veya entegrasyon işlemleri iptal edilebilir. Sürekli entegrasyon sayesinde klasik yaklaşımda elle yapılan bu işlemler otomatik ve kimseye bağımlı kalmadan yapılabilir.

Sürekli Teslim

Sürekli teslim, uygulamanın entegrasyon sürecinde başarılı olması durumunda son testlerin gerçekleştirildiği ve üretim ortamına hazırlandığı ortamdır. Derleme aşamasından sonra tüm kod düzeyindeki değişiklikler bir ön üretim ya da test ortamına dağıtılarak sürekli entegrasyon sağlanır. Sürekli teslim yapısı düzgün ve sağlıklı bir biçimde kurgulanıp devreye alındığında geliştiriciler için her zaman düzgün biçimde testi yapılmış, çeşitli kural ve politikalardan başarı ile geçmiş dağıtıma hazır hâlde bir uygulama üretilmiş olacaktır.

Sürüm Yönetimi ve Denetim

Ekipler tarafından geliştirilen yazılımlara ait kodların ve yapıların gözden geçirilmesi ve kontrol edilmesi sürecidir. Genellikle Git benzeri sürüm kontrol araçları ile birden fazla geliştiricinin birlikte çalışabilmesine olanak tanımaktadır. Bu tür sistemler bir kod bloğundaki tüm değişikliklerin izlenmesi, birleştirilmesini veya çıkarılmasını, daha eski sürümlere kolaylıkla geçişlerin yapılabilmesini sağlar. Sürüm yönetimi, sürekli entegrasyon ve sürekli teslim sürecinin ayrılmaz bir parçasıdır.

Kod Olarak Altyapı

Kod olarak altyapı, klasik yaklaşımda elle gerçekleştirilen tüm alt yapı ve sistem yönetiminin, yazılım kodları gibi yazılmasına ve yönetilmesine olanak tanır. Aynı şekilde bir kod geliştirimi gibi gözden geçirilebilir, iyileştirilebilir ve dağıtımları farklı sistemlerde şablon olarak kullanılabilir. Tüm sistem ve altyapı süreçleri otomatikleştirilerek ciddi biz hız avantajı ve güvenirlik sağlanabilir. Canlı ve test ortamları aynı şablon üzerinden kurulup çoğaltılabilir, bu şekilde ekipler daha esnek ve rahat bir çalışma ortamına kavuşabilir. Bu süreçte aynı zamanda çeşitli politikalar ile uyumluluklar da kontrol edilebilir veya doğrulanabilir. Örneğin, bir sistem PCI-DSS veya HIPAA uyumlu olmak zorunda ise bu şablonlarda bu tür politika ve kurallar yer alabilir.

Çevik Yazılım Geliştirme

Çevik yazılım temelinde müşteri ve kullanıcı geri bildirimlerine hızlı şekilde cevap verebilmek yatmaktadır. Kısa sürüm döngüleri sayesinde müşteri ve kullanıcıların istekleri en kısa zamanda teslim edilebilir. Bu sistemin yönetiminde genellikle Kanban ve Scrum çerçevesi kullanılmaktadır.

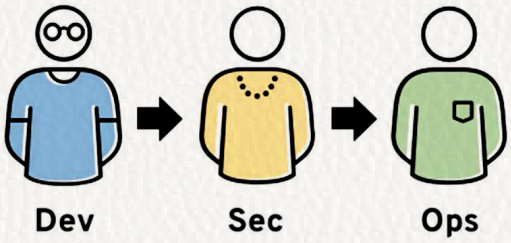
Sürekli İzleme ve Günlük Kayıtları

Sürekli izleme, bir uygulamaya ilişkin yaşam döngüsü boyunca üretilen hata ve performans gibi kayıtların; ekranlar, izleme araçları veya raporlar ile görünürlüğünü ifade etmektedir. Bu toplanan veriler analiz edilerek bir yaklaşım sergilenebilir. Örneğin, ekipler hataları önceden tahmin edip gerekli düzeltmeleri yapabilir veya performans sorunlarını çok daha önceden tespit ederek iyi bir müşteri deneyimi sunabilir. Uygulama yaşam döngüsündeki görünürlük ne kadar iyi ise verim o kadar yüksek olacaktır.

12.3. DEVSECOPS

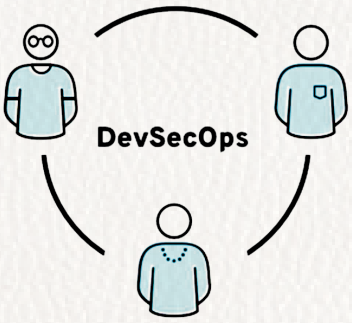
12.3.1. DevSecOps'un Genel Tanımı

DevSecOps, uygulama geliştirme yaşam döngüsünde baştan sona kadar olan süreç ve sonrası dâhil güvenliğin benimsemesi ile olası güvenlik açıklarının her düzeyde tespit veya tahmin edilmesine ve giderilmesine imkân sağlayan bir metodolojidir. DevOps aşamalarına güvenliğin dâhil edilmesidir de denebilir. Klasik yaklaşımda her bir görev farklı rollerde yer alırken, DevSecOps tıpkı DevOps'ta olduğu gibi görevlerin birbiri içerisine geçmesine olanak tanır.



Şekil 12.2. Klasik Yaklaşım [4]

Diğer bir ifadeyle, yazılım geliştirme yaşam döngüsünde yer alan her kişi ve birimin güvenlikten sorumlu olması, özünde operasyonları ve geliştirmeyi güvenlik işlevleriyle bir araya getirmesidir. Bir kuruluşun veya kurumun geliştiriciler, güvenlik ekibi ve operasyon ekibi arasındaki boşluğu en az düzeye indirmesin sağlayan bir kültür ve uygulamalar bütünü tanımı da yapılabilir. Her ne kadar Şekil 12.2'de gösterilen klasik yaklaşım kullanılsa da DevSecOps'ta önemli olan Şekil 12.3'te gösterildiği gibi her kişinin her işten sorumlu olduğu bir çalışma kültürüne evrilmektir.



Şekil 12.3. DevSecOps Yaklaşımı [4]

DevSecOps yaklaşımı için tek bir tip yöntemden söz edilemez. Her bir kuruluşun veya kurumun DevSecOps'u kendi kültürüne ve benzersiz süreçlerine, ürünlerine, güvenlik gereksinimlerine ve operasyonel prosedürlerine göre uyarlaması gerekir. DevSecOps'un benimsenmesi, kuruluşların kültürlerini değiştirmelerini, mevcut süreçleri geliştirmelerini, yeni teknolojileri benimsemelerini ve yönetişimi güçlendirmelerini zorunlu kılmaktadır.

Bu bölümde DevSecOps yaşam döngüsü, destek süreçleri ve DevSecOps ekosistemi üzerine durulacaktır.

12.3.2. DevSecOps Neden Bu Kadar Önemli?

Daha önceki DevOps konusunda da belirtildiği gibi bilgi teknolojileri hızlı bir değişim geçirmekte buna paralel olarak yazılım süreçleri ve geliştirimi de aynı hızla değişmektedir. Özellikle bulut teknolojilerinin yaygınlaşması ile hız ve çeviklik artarken aynı zamanda maliyet unsurlarında da bir azalma söz konusu olduğu görülmektedir.

Uygulamaların artık bulut mimarileri üstünden dağıtılabilmesi, uygulama ve yazılımların daha hızlı ve daha geniş ölçekte bir alana sunulabilmesine, bunlar ile birlikte DevOps süreçlerinin geliştirime dâhil edilmesi ile daha çok güncelleme ve yeni sürümün hızlı biçimde sahaya çıkmasına imkân sağlamaktadır.

Tüm bunlar bir anlamda mükemmel bir tablo çizse de DevOps süreçlerindeki izleme ve güvenlik araçlarının yetersizliği nedeni ile birçok güvenlik problemi de ortaya çıkmaktadır. DevOps'ta genel amaç çevik ve hızlı biçimde yeni sürümler ortaya çıkarmak üzerine odaklandığından güvenlik genellikle son aşamalara bırakılmış, bu da sonuçta ciddi sorun ve maliyetlere neden olmuştur.

Bu sorunu ortadan kaldırmak için DevSecOps metodolojisi geliştirilmiş ve güvenliğin de hızlı ve çevik geliştirimde yer bulması hedeflenmiştir.

12.3.3. DevSecOps'un Faydaları

Baştan sona kadar otomatikleştirilmiş ve denetimi sağlanmış süreçler, tıpkı DevOps'ta olduğu gibi riskleri ve hataları en az düzeye indirerek ve temel güvenlik sorunlarının olası en erken zamanda tespit edilmesini sağlayarak sürece dâhil olmadan engellenmesine imkân tanıyacaktır. Diğer taraftan güvenlik araçları ve altyapıları ile ilgili birçok konfigürasyon bir seferde oluşturulup otomatikleştirileceğinden ciddi bir zaman kazanılacaktır. Bu kapsamda aşağıdaki temel faydalardan bahsedilebilir.

Maliyet Faydası

Güvenliği baştan tasarlanmış ve sürece dâhil edilmiş bir sistemde hata ve sorunlar geliştirim sürecinde tespit edilebilir. Süreç içerisinde bulunan ve düzeltilen hatalar son aşamada yapılacak düzeltmelerden her şekilde daha avantajlı ve daha az maliyetli bir iştir.

Olay Sonrası Hızlı Toparlanma Avantajı

Herhangi bir güvenlik ihlali ya da olayı sonrasında, daha önceden hazırlanmış ve sürece dâhil edilmiş şablonlar ve sistemler sayesinden hızlı biçimde toparlanma ve işi devam ettirme şansı olur.

Güvenlik İzleme, Denetleme ve Uyarı Sistemleri ile Anında Haberdar Olma

Güvenlik denetimi, izleme ve bildirim sistemleri, otomasyona dâhil edilerek sürekli olarak sistemler izlenebilir, saldırı veya ihlal durumunda çeşitli uyarılar üretilebilir veya otomatikleştirilmiş süreçler devreye alınabilir. Bu sayede müdahale süresi kısalır ve en az şekilde zarar ile saldırı bertaraf edilebilir.

Tasarım Gereği Güvenliğin Benimsenmesine Olan Katkısı

Tasarım gereği güvenlik, birçok güvenlik standardı üzerinde güvenlik ve uyumluluk yaklaşımı olarak tarif edilebilir. DevSecOps, kodların otomatik biçimde güvenli yazılım gözden geçirmelerinin yapılması, otomatik uygulama güvenlik testlerinin kullanılması ile geliştiricilerin de güvenli tasarım modellerine uygum sağlamasına yardımcı olmaktadır.

12.4. DEVSECOPS TEMELLERİ

12.4.1. Temel İlkeler

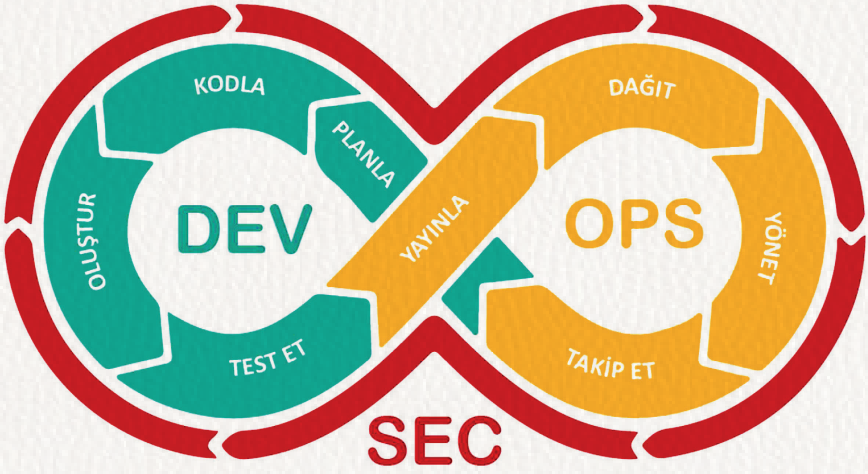
Başarılı bir DevSecOps yaklaşımını uygulamanın ilkeleri şöyle listelenebilir:

- Süreci engelleyecek veya aksatacak tüm faktörler (insanın kendisi de dâhil) ve el ile yürütülen eylemler kaldırılmalıdır.
- Mümkün olduğunca geliştirme ve dağıtım faaliyetleri otomatikleştirilmelidir.
- Planlama ve gereksinimlerden dağıtım ve operasyonlara kadar genel ve bilinen araçları benimsenmelidir.
- Çevik yazılım ilkelerinden yararlanılmalı ve büyük/karmaşık sürümlere kıyasla küçük, versiyonlu ve sık güncellemeler tercih edilmelidir.
- Tek bir yetenek üzerinde uzmanlaşmak yerine yazılım yaşam döngüsü boyunca çapraz fonksiyonel beceriler geliştirmeli, siber güvenlik ve operasyonel yetenekler de arttırılmalıdır.
- Mevcut altyapının güvenlik riskleri ölçülmeli ve değerlendirilmeli, böylece yazılım uygulamalarına yönelik toplam riskler ve etkiler anlaşılmalıdır.

- Değişmez ve önceden konfigürasyonu ve bileşenleri hazırlanmış altyapı dağıtım yöntemleri benimsenmelidir. Değişmez altyapı kavramı, devreye alınan bileşenlerin mevcut bulunduğu ortamda güncellenmesi veya ayarlanması yerine tamamen değiştirildiği bir BT stratejisidir. Değişmez altyapının dağıtılması, tutarlı ve öngörülebilir sonuçlar elde etmek için ortak altyapı bileşenlerinin standartlaştırılmasını gerektirir.

12.4.2. DevSecOps Yaşam Döngüsü

DevSecOps yazılımı yaşam döngüsü aşamaları genellikle Şekil 12.4'te gösterildiği gibidir. Sekiz aşamadan meydana gelmektedir. Bunlar; planlama (İng. plan), Kodlama (İng. develop), oluşturma (İng. build), test veya doğrulama (İng. test), yayınlama (İng. release), dağıtma (İng. deploy), yönetme (İng. operate) ve izleme veya takip etme (İng. monitor) olarak belirtilebilir. Güvenlik, tüm bu aşama ve süreçlerin içerisinde yer almaktadır.



Şekil 12.4. DevSecOps Yaşam Döngüsü [11]

DevSecOps ile, yazılım geliştirme yaşam döngüsü blok hâlinde –monolitik– doğrusal bir süreç olmaktan çıkmıştır. Şelale modeli yapısındaki bir ürün teslimi yaklaşımından çok, daha küçük ama daha sık teslimatlara yer verilir, böylece ihtiyaç duyulması hâlinde yapı veya kodlarda istenilen şekilde değişikliklerin yapılması daha da kolaylaşmaktadır.

Her küçük teslimat, hızlı ve sürekli olması adına, entegrasyonlar ve minimum insan müdahalesiyle otomatik bir süreçle gerçekleştirilir. DevSecOps yaşam döngüsü farklı senaryolara göre uyarlanabilir ve sürekli iyileştirme için birçok geri besleme döngüsüne de sahiptir.

12.4.3. DevSecOps'ta Katmanlar

Şekil 12.5'te görüldüğü gibi DevSecOps genel olarak "İnsan, Yönetişim, Süreç ve Teknoloji" olarak dört katman tarafından desteklenmektedir.

Şekil 12.5. DevSecOps Katmanları [13]

Her kuruluş için DevSecOps uygulaması, DevSecOps felsefesinin organizasyon bünyesine katılmasıyla başarılı olabilir. Bu, süreci otomatikleştirmek ve tutarlı yönetişim uygulamak için yeni iş birliği süreçleri, teknolojileri ve araçlarının geliştirilmesi ile birlikte organizasyon kültüründe bir değişikliğe yol açar. Başarılı olmak için bir projenin dört alanda da ilerlemesi gerekir:

1. İnsanlar DevSecOps uygulamasının başlangıç noktasıdır. Ekiplerin uygun eğitimi ve yeniden yapılandırılmasını sağlayarak güvenlik bir engel olmaktan ziyade bir düşünce yapısı hâline gelecektir.
2. Yönetişim, yazılım yaşam döngüsü boyunca görev programıyla ilişkili riskleri aktif olarak değerlendiren ve yöneten bir yapıdır. Yönetişim faaliyetleri süreklilik içerisinde, operasyonlar ve izleme de dâhil olmak üzere yazılım yaşam döngüsü boyunca devam eder.

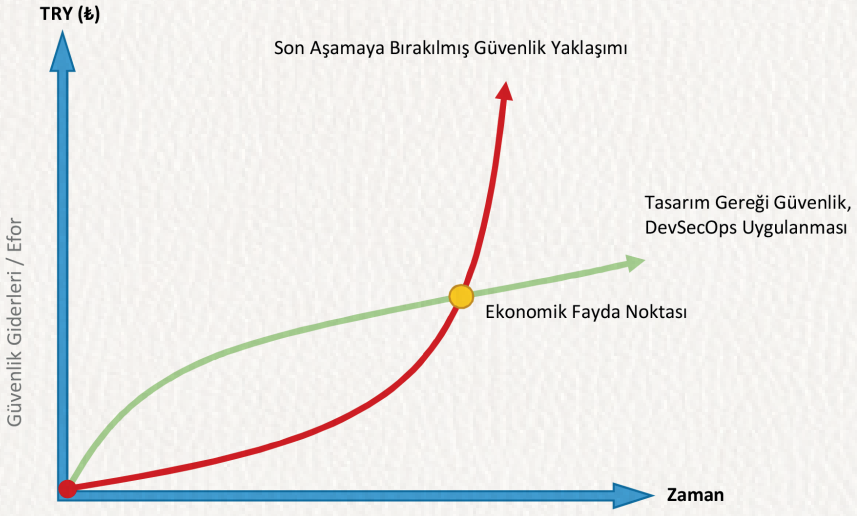
3. DevSecOps, iş birliğini kolaylaştırmak ve bir bütün olarak daha güvenli geliştirme süreçlerine ulaşmak için bir kuruluşun ortak süreçlerini hizalamayı ve uygulamayı hedeflemektedir.
4. Teknolojiler, insanların kurumsal saldırı yüzeyini azaltmayı ve teknik güvenlik borcunun etkin yönetimini sağlamayı amaçlayan DevSecOps süreçlerini yürütmelerini sağlar.

Bu kavramlar aşağıda daha detaylı incelenmiştir.

İnsan

Hangi teknoloji olursa olsun, en zayıf halka her zaman insan faktörüdür. Bu durum aslında DevSecOps uygulaması için de bir çıkış noktası olmaktadır. Bir şirketin tüm seviyelerinde değişen alışkanlıklar ve farkındalık yaratmak kolay bir iş değildir ve kültür değişecek ise yukarıdan aşağıya bir yaklaşıma sahip olmak gerekmektedir.

Güvenlik, bu kültür değişikliğini kolaylaştırmak için münhasır olmaktan kapsayıcı olmaktan yana olmalıdır. DevSecOps gibi güvenlik ekiplerini geliştirme ekiplerine entegre ederek şirketler, "güvenlik açısından" kod, yazılım veya uygulamanın kalitesi hakkında daha erken geri bildirim alacak ve böylece bu düzeltmelerin uygulanmasıyla ilgili maliyetleri azaltacaktır.



Şekil 12.6. Güvenlikte Zaman/Maliyet Grafiği [14]

Bu noktada "Güvenlik Liderleri", Uygulama Güvenliği ve Güvenlik Operasyonlarına odaklanan çok işlevli bir ekip oluşturmanın ilk adımı olduklarından DevSecOps metodolojisinin önemli bir öğesidir. Güvenliğin etkili olabilmesi için, güvenlik personeli yazılım geliştirim yaşam döngüsüne mümkün olduğunca erken dâhil edilmelidir. Bunu yapmanın bir yolu, geliştirme ekibindeki güvenlik şampiyonlarını (liderleri) eğitmekten geçmektedir. Bu sayede Şekil 12.6'da görüldüğü gibi fayda/maliyet açısından etkin bir güvenlik sağlanmış olur.

Güvenlik liderlerinin bazı önemli görevleri aşağıdaki gibi sıralanabilir:

- Güvenlik aktif geliştirim veya gözden geçirmelerde engelleyici unsur olmamalıdır.
- Karar verici bir rol üstlenmelidir.
- Yazılım güvenlik takımları ile birlikte hareket etmelidir.
- Kalite Güvence ve Test faaliyetlerinde yardımcı olmalıdır.
- Sürekli entegrasyon süreci için geliştirime katkıda bulunmalıdır.
- Güncel güvenlik tehditlerini ve gelişmelerini takip etmeli ve güncel kalmalıdır.
- Uygulama güvenliği ile ilgili metot, kaynak ve dokümanları ekip içerisinde yaygınlaştırmalıdır.

Tüm bunlarla birlikte güvenlikte eğitim önemli bir rol oynamaktadır. Ekiplerin sürekli güncel kalmalarına yardımcı olacak çeşitli yazılım güvenlik eğitimleri organize edilmeli ve ekiplerin bu eğitimleri katılmaları için teşvik edilmelidir.

Bunların haricinde kurum ve işletmeler, aşağıdaki felsefeleri ve fikirleri benimsemeli ve günlük faaliyetlerine ve yazılım yaşam döngüsü yönetim süreçlerine dâhil etmelidir:

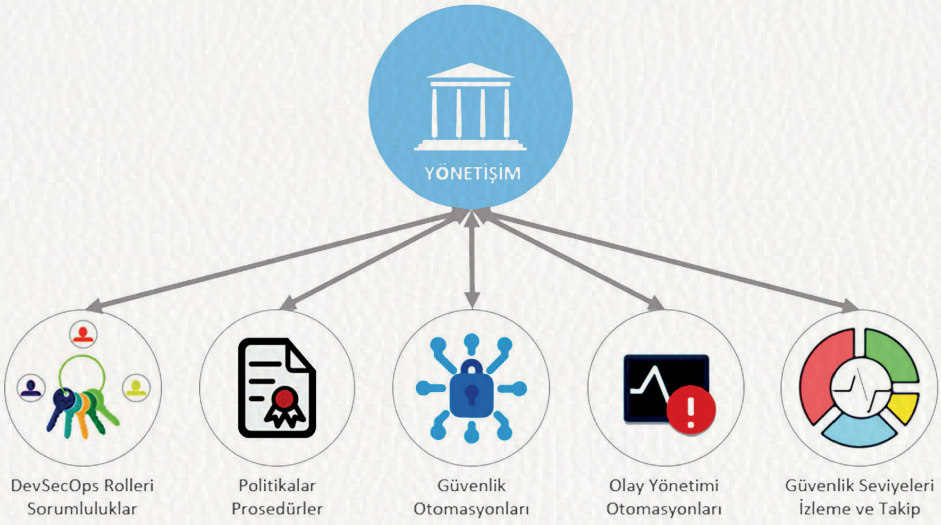
- Bütünsel bir bakış açısı kazanılmalıdır. Yazılım geliştirme, güvenlik ve operasyonların sorumluluğunu paylaşmak için organizasyon yapısında ve kültüründe değişiklikler yapılmalıdır. Ekipler DevSecOps kavramları ve yeni teknolojilere uygun kapsamda eğitimler ile desteklenmeli ve geliştirilmelidir. Bir süreç içerisinde tüm ekiplerin ve paydaşların katılımı sağlanmalıdır.

- Yazılım yaşam döngüsünün tüm aşamalarında ekip iletişimi ve iş birliği arttırılmaya çalışılmalıdır.
- İş birliğini mümkün kılmak için, güvenlik uyarıları veya kalite güvence raporları gibi işlem yapılabilir nitelikteki güvenlik ve kalite güvence bilgileri, her yazılım yaşam döngüsü aşamasındaki ekipler tarafından otomatik olarak kullanılabilir ve erişilebilir olmalıdır.
- İşletme veya kurum genelindeki olumlu ve olumsuz olaylarla ilgili eylem sonrası raporları paylaşarak bir güvenlik kültürü oluşturulmalıdır. Ekipler, DevSecOps uygulamasının bir parçası olarak sistem tasarımını geliştirmek, uygulamayı daha güvenli hâle getirmek ve olaylara karşı verilecek yanıt ve eylem yeteneğini geliştirmek için hem başarı hem de başarısızlığı öğrenme fırsatları olarak kullanmalıdır.
- Daha az ve daha büyük değişiklikler yerine daha çok ve küçük, artımlı değişiklikler yapılmalıdır. Küçük değişikliklerin kapsamı daha sınırlı olacağından yönetimi de daha kolay olacaktır.
- Beklenmedik ve öngörülmedik şekilde ortaya çıkabilecek değişiklik ve yeniliklere hızlı ve doğru cevap verebilmek için geri bildirimleri ve müşteri odaklı değişimleri benimsenmelidir.
- Birikmiş teknik borçların sürekli olarak giderilmesini veya sahiplenilmesini sağlamak için devamlı olacak şekilde kod yeniden düzenleme/gözden geçirme faaliyetleri için bir plan ve bütçe belirlenmelidir.

Yönetişim

Yönetişim, yazılım yaşam döngüsü boyunca görev programıyla ilişkili riskleri aktif olarak değerlendiren ve yöneten bir yapıdır. Şekil 12.7'de gösterilen yönetişim faaliyetleri süreklilik içerisinde, operasyonlar ve izleme de dâhil olmak üzere yazılım yaşam döngüsü boyunca devam eder. DevSecOps birçok yönetişim faaliyetini kolaylaştırabilir ve otomatikleştirebilir.

DevSecOps'un yönetişim hedefi, daha büyük stratejik hedefleri dengelemek için hem "yukarıdan aşağıya" hem de "aşağıdan yukarıya" olmalıdır. Hızla değişen dünyaya ayak uydurmak için yönetişim için sürekli süreç iyileştirme, mümkün olan her yerde basitleştirme ve otomatikleştirme fırsatları aramak, bir zorunluluk hâlini almıştır.



Şekil 12.7. Yönetişimin Yaşam Döngüsü Faaliyetleri [13]

Çok işlevli DevOps ekiplerinde iyi tanımlanmış roller ve sorumluluklar oluşturmak bir gerekliliktir. Bu yüksek verimli operasyonların yapılmasına imkân tanır. DevSecOps'a özgü politika ve prosedürlerin oluşturulması ve yayınlanması, kuruluşların bir DevOps ortamında uygulama geliştirme hızına ayak uydurmasına olanak tanıyacaktır.

DevSecOps hattındaki otomatik güvenlik ve test araçları, insan hatası nedeniyle güvenlik açıklarını ve güvenlik kusurlarını azaltarak genel güvenliği en üst seviyelere çıkartacaktır. DevSecOps'taki güvenlik izleme ve bildirim sistemleri, yazılım geliştirme yaşam döngüsü boyunca otomatik raporlama denetimi sağlar ve bu da yasal uyumluluk raporlamasını (ISO 27001 v.b.) kolaylaştırmaktadır. Güvenlik metriklerini sürekli izlemek, DevOps ekiplerinin güvenlik kararlarını tutarlı bir şekilde iyileştirmelerine ve oyunun zirvesinde kalmasına olanak tanır.

Süreç

Her bir sistem ve işlem kendi çerçevesinde özeldir. Bu nedenle her yazılım yaşam döngüsünün kendine has yönetim süreçlerinin olması kaçınılmazdır. Ortamın yapısı ve çeşitliliği, sistem tasarımı ve büyüklüğü, sistemin mimari

yapısı, yazılım tasarım modelleri, risk belirteçleri ve düzeyleri gibi faktörlerin tamamı bu süreçlerde etkili birer faktördür.

Örnek vermek gerekirse, bir web uygulamasında test, yayına alma, izleme vb. tüm süreçler otomatikleştirilebilirken, gömülü sistemlerde bazı test ve prosedürler otomatikleştirilemeyebilir. Bu yüzden her iki süreç farklı ele alınmalıdır.

Bir DevSecOps sürecini başarılı bir şekilde oturtabilmek için, birden fazla aşamaya yayılmış bir yaklaşım izlenebilir. Örneğin, otomatikleştirmesi kolay olan görevler ile başlanarak, ardından daha karmaşık ve zor görevleri de dâhil ederek DevSecOps oluşturulabilir.

Tüm süreci bir seferde DevSecOps'a geçirmek yerine ilk aşamada sadece derleme ve test aşamaları ile başlamak diğer aşamalar için de bir deneyim oluşturacaktır. Yeterli sonuç ve beklenti karşılandığında sonraki süreçlerde dâhil edilerek tam bir DevSecOps geçişi yapılabilir.

Süreç tasarımı için "herkese uyan tek bir çözüm" ne yazık ki mümkün değildir. Her yazılım ekibinin kendine özgü gereksinimleri ve kısıtlamaları veya ihtiyaçları bulunmaktadır. Başlangıç için aşağıdaki adımlar en iyi uygulama listesi olarak referans alınabilir:

- Süreç tasarımı, ekiplerin ortak bir çabası ile mümkün olur.
- Süreçlerin çoğu araçlar ve teknolojilerle otomatikleştirilebilir olmalıdır.
- DevSecOps yaşam döngüsü yinelemeli bir kapalı döngüdür. İlk başlarda insan müdahalesi çoğunlukta olsa da daha sonra sürecin olgunluk düzeyine ve ekibin otomasyondaki güven düzeyine bağlı olarak, insan müdahalesi gerektiren yerlerin otomatikleştirilmesi tercih edilmelidir.
- Yetki merkezleri ve otoriteleri, yetkilendirme süreçlerini de mümkün olduğunca otomatikleştirmeyi düşünmelidir.

Teknoloji

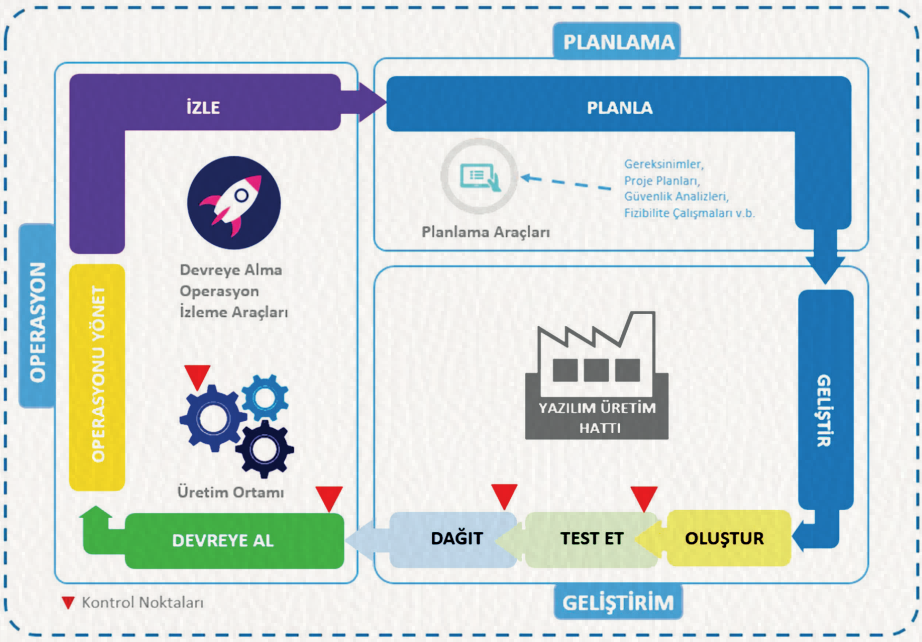
Mevcut DevSecOps araçları sayesinde yazılım yaşam döngüsünde yer alan birçok görev insan müdahalesine gerek duymadan otomatik hâle ge-

tirilebilmektedir. Birlikte çalışmaya imkân tanıyan iş birliği ve iletişim araçları gibi diğer DevSecOps araçları, verimliliği arttırmak için insan etkileşimini kolaylaştırır ve teşvik eder. Bazı DevSecOps araçları, belirli bir yaşam döngüsü aşamasında bir etkinliğe yardımcı olmayı amaçlayabilir. Örneğin, geliştirme aşaması için bir Tümleşik Geliştirme Ortamı (IDE) eklentisi veya derleme aşaması için statik uygulama güvenlik sınama ve test araçları, bağımlı paket güvenlik denetimleri işletilebilir. DevSecOps araçları ile tek seferde bir bileşeni veya sistemi elle ayarlamak yerine yapılandırma dosyalarından faydalanılabilir ve böylece tekrar tekrar kullanılabilir.

Altyapı yapılandırma dosyaları, DevSecOps aracı yapılandırma komut dosyaları ve uygulama çalışma zamanı yapılandırma komut dosyaları Altyapı olarak Kod (IaC) olarak adlandırılır. IaC ile aynı yaklaşımı benimseyen güvenlik ekipleri, güvenlik politikalarını doğrudan yapılandırma koduna programlamanın yanı sıra, Kod olarak Güvenlik (SaC) olarak adlandırılan güvenlik uyumluluğu denetimi ve kodunu kod olarak uygular. Hem IaC hem de SaC yazılım olarak değerlendirilir ve tasarım, geliştirme, sürüm kontrolü, emsal değerlendirmesi, statik analiz ve test gibi titiz yazılım geliştirme süreçlerinden geçer.

12.5. DEVSECOPS HATTI

Tüm DevSecOps yaşam döngüsü boyunca yer alan etkinlikleri ve işlemleri yönetmek, izlemek ve test etmek için birçok araç kullanılmaktadır. Bu araçlar ihtiyaç duyulan tüm etkinlikleri de otomatikleştirerek bağımlılıkları ortadan kaldırmayı amaçlar. Hat (İng. pipeline) olarak adlandırabileceğimiz bu süreçte tüm işlemler bir düzen içerisinde ve belirli bir ilişki bağı ile birbirini izlemektedir. Tüm bu süreçlerin yer aldığı akış Şekil 12.8'de gösterilmiştir. Bu akışta genel olarak üç farklı alt aşamadan bahsedilebilir. Bunlar "Planlama", "Geliştirme" ve "Üretim" olarak sınıflandırılabilir. Her bir aşama için farklı araçlar ve altyapılar kullanılması söz konusu olabilmektedir. DevSecOps'tan bahsederken DevOps ile birlikte düşünmek gerekir. Aşağıdaki grafik temel düzeyde bu sistemi göstermektedir.



Şekil 12.8. DevSecOps Hattı Yaşam Döngüsü [17]

Planlama

Planlama aşaması, proje ile ilgili maliyetlerin, zaman çizelgelerinin, risklerin, kalite beklentilerinin ve sorunların yönetilmesinde yardımcı olan faaliyetleri içerir. Bu faaliyetler arasında iş gereksinimi değerlendirmesi ve belirlenmesi, proje planının oluşturulması, risk ve fizibilite analizlerinin yapılması, iş gereksinimlerinin toplanması, sistem tasarımının yapılması, iş süreçlerinin oluşturması, DevSecOps'un tasarımı gibi konular yer almaktadır. Basit anlamda güvenlik analizlerinin yapılması, testlerin nerede, nasıl ve ne zaman yapılacağı ile ilgili senaryoların ve planların oluşturulması, test kabul kriterlerinin belirlenmesi, politikaların ve tehdit modellerinin oluşturulması aşamalarını içermektedir.

DevSecOps'nun yaşam döngüsü boyunca plan aşaması tekrarlanmaktadır. Kritik ve en çok öneme sahip fakat en düşük kabul edilebilir veya uygulanabilir bir düzeyde ürün geliştirmek amaçlanmalıdır. Ardından, mümkün oldu-

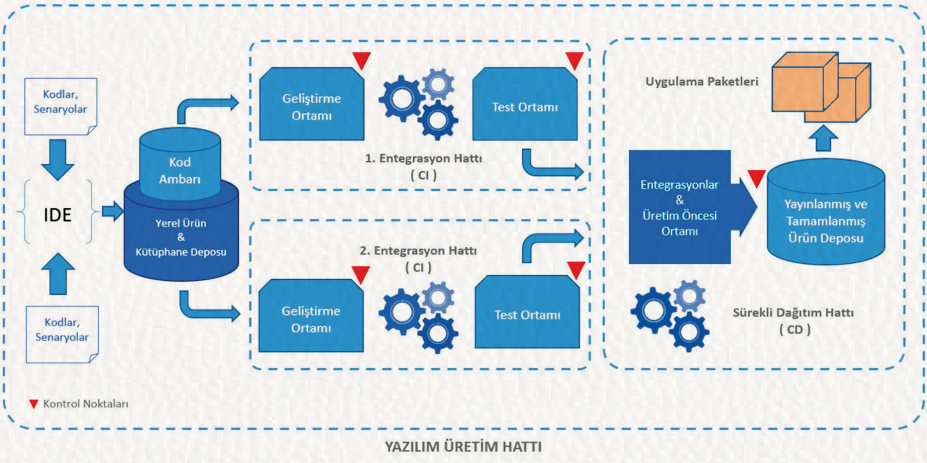
ğunca hızlı biçimde geri bildirim döngüsü sürecine girilmelidir, bu yöntem aynı zamanda "Yalın Geliştirme" metodolojisinde de önerilmektedir.

DevSecOps'ta planlama yapısı, bir dizi iletişim, iş birliği, proje yönetimi ve değişiklik yönetimi araçlarını kullanarak plan aşamasındaki faaliyetleri destekler. Bu aşamada, iş akışlarının tam olarak otomatikleştirilmesi söz konusu olmasa da kullanılan araçlar ile insan etkileşimlerine destek olur ve ekip verimliliğini arttırır.

Geliştirim

Şekil 12.9'da gösterilen bir yazılım üretim hattı, insan müdahalesinin en az olduğu, bir dizi araç, işlem iş akışı, komut dosyaları, senaryolar ve sistemler ile donatılmış birden fazla hat içerir. Geliştirme, oluşturma, test etme, yayınlama ve teslim etme aşamalarındaki faaliyetleri otomatik hâle getirir.

Yazılım üretim hattında kurulan ortamlar ve sistemler, "Kod Olarak Altyapı (İng. Infrastructure as a Code – IaC)" komut dosyalarıyla düzenlenmelidir. Yazılım üretim hattı tasarlanırken birden fazla proje için yazılım üretimini otomatikleştirebilecek yeteneklerde olmalıdır. Pratikte farklı ortam ve uygulamalar için farklı üretim hatları oluşturulması önerilmektedir. Bir uygulama farklı üretim hatlarından gelen çıktılar ile bütünleştirilebilir.



Şekil 12.9. Yazılım Üretim Hattındaki Temel Mimari [17]

Yazılım Üretim Hattı, uygulama kodlarını ve altyapı olarak kodları geliştiren geliştirme ekipleri, test senaryolarını geliştiren kod kalite kontrol ekipleri ve "Kod Olarak Güvenlik" yapılarını geliştiren güvenlik ekipleri ile başlar.

"Yazılım Üretim Hattı" boyunca, mümkün ise OCI (Open Container Initative bkz: https://opencontainers.org/faq/) standartları ile uyumlu veya kurumsal olarak güvenliği arttırılmış, test edilmiş ve güvenlik ekipleri tarafından onaylanmış kapsayıcılar (İng. containers) kullanmalıdır.

Yeni geliştirilen kod ve komut dosyaları Yazılım Fabrikası'nın kod deposuna veya ambarına işlendiğinde, üretim hattı otomasyonu devreye girer. Birden fazla sürekli entegrasyon (CI) hattı olabilir. Örnek vermek gerekirse, sürekli entegrasyon hatlarından biri JavaScript komutlarını işlerken, diğeri bir web uygulaması için farklı araç ve komutlar ile ön yüz sistemini işleyebilir. Sürekli entegrasyon hattı, kodu oluşturarak ve yerel ürün deposundan bağımlılıkları (üçüncü taraf kütüphaneler gibi) ilgili koda ekleyerek alt sisteme sürekli entegrasyon yoluyla rehberlik eder.

Ayrıca, birim testleri, statik kod analizi, fonksiyonel testler, arayüz testleri, dinamik kod analizi vb. gibi geliştirme ve test ortamlarında testler gerçekleştirir.

Sürekli entegrasyon hattı kontrol kapıları (İng. control gates) politikalarını geçen alt sistemler, üretim öncesi ortama taşınır. Bu aşamada "Sürekli Dağıtım Hattı" kontrolü devralır. Bu ortamda performans testleri, kabul testi, güvenlik uyum taraması vb. gibi daha fazla kapsamlı test ve güvenlik taraması yapılır. Sürekli Dağıtım Hattı, kontrol noktası veya kapısı politikaları karşılandığında nihai ürün paketini yayınlanan ürün deposuna gönderir ve teslim eder.

Yazılım Üretim Hattının bu şekilde planlanması ve işletilmesi birçok fayda sağlamaktadır. Bunlardan bazıları şöyle sıralanabilir:

- Nihai ürünün kalitesi ve tutarlılığı garanti edilmiş olur.

- Ürünün müşteriye ulaştırılması için geçen süre kısalır.
- Verimlilik artar, hatalar azalır, maliyet düşer.
- Raporlama ve süreç analizleri kolaylaşır.
- Görünürlük artar ve erken müdahale imkânı yaratılır.
- Yönetişim faaliyetleri basitleşir, daha kolay yönetilir hâle gelir.

Operasyon

Bir önceki süreçte yayınlanmış ve tamamlanmış olan yazılım ürünü, yayınlanmış ve tamamlanmış ürün havuzundan alınır ve dağıtılır. Bu esnada gerçekleşen tüm işlemler, işlem monitörleri ve güvenlik monitörleri ile sürekli takip edilir.

Üretim operasyon araçları, dağıtım, operasyonlar ve izleme faaliyetlerini kolaylaştırmayı ve otomatikleştirmeyi amaçlamaktadır. Araçlar, sistemin fonksiyonel gereksinimlerine ve bunların üretim ortamı altyapısına uygunluğuna göre seçilmelidir.

12.6. DEVSECOPS ARAÇLARI

Planlama Adımı

Aşağıdaki listede planlama sürecine yardımcı olabilecek bazı araçları listelemektedir. Bu araçlar bir DevSecOps ekosisteminde yapılandırma ve değişiklik yönetimi, sistem ve yazılım tasarımları, kalite ve güvenlik testleri için gerekli olan planlama destek yazılımlarıdır. Bu araçların yönetim ve kullanımında politika ve prosedürlerin uygulanması gerekebilir.

Uygulama Yaşam Döngüsü Yönetim Araçları

Uygulama yaşam döngüsü (UYD) yönetimi, bir uygulamanın yaşam döngüsünü, tasarımından kullanım ömrünün sonuna kadar yöneten kişiler, araçlar ve süreçlerdir. UYD; proje yönetimi, gereksinim yönetimi, yazılım geliştirme, test ve kalite güvencesi, dağıtım ve bakım gibi çeşitli disiplinlerden oluşur.

Uygulama yaşam döngüsü yönetimi, yazılımın zaman içinde yönetilmesine yardımcı olurken yazılım geliştirme için de bir çerçeve sağlar. UYD uygulamalarını takip etmek, bir fikri uygulamaya dönüştürmek için hafif, önceden oluşturulmuş bir plan kullanır.

Aşağıda tüm bu süreçlerin yönetilmesinde kullanılabilecek bazı araç ve yazılımlar verilmiştir:

- JIRA
- Mingle
- Trello
- VisualStudio TFS
- Azure DevOps
- Basecamp
- AWS CodePipeline

Takım ve Ekip Yönetim Araçları

Mutlaka sesli ve görüntülü görüşme yeteneği olan araçlar tercih edilmelidir. Dosya ve ekran paylaşımı yapılabilen, çeşitli wiki özelliklerine sahip, takvim vb. uygulamaları olan araçlar planlama aşamasında gereken tüm ihtiyaçları sağlayacaktır. Bu tür araçlar takım ve ekiplerin motivasyon ve verimliliğinde ciddi bir artış sağlayacaktır. Bu araçlara örnek olarak aşağıda listelenenler verilebilir:

- Slack
- HipChat
- Flowdock
- Microsoft Teams
- Nestor
- Lita

Bilgi ve Tecrübe Paylaşım Araçları

Takımların veya ekiplerin gerek önceden edinmiş oldukları bilgi ve tecrübeler gerekse mevcut geliştirim aşamalarında edindikleri tecrübe ve bilgi birikimle-

rini paylaşmalarına, tartışmalarına ve soru-cevap şeklinde çözüm aramalarına olanak tanıyan yazılım veya uygulamalardır. Bu araçlara örnek olarak aşağıda listelenenler verilebilir:

- JIRA
- Mingle
- Trello
- VisualStudio TFS
- Azure DevOps
- Basecamp

Sorun ve Hata İzleme Araçları

DevOps'daki araçlara benzer şekilde kullanılabilen araçlardır. Sorun izleme araçları, sürekli entegrasyon/sürekli teslim boru hatlarıda meydana gelen değişiklikleri ve güvenlik sorunlarının takip edilebilmesine imkân tanır. Aşağıda, mevcut en popüler araçlardan bazıları verilmiştir:

- WhiteSource
- Azure DevOps
- Bugzilla
- Jira
- Mantis
- Trac
- OverOps
- YouTrack

Tehdit Modelleme Araçları

DevSecOps tehdit modellemesi, güvenliğin gelişimin ilk aşamalarından itibaren dikkate alınmasını sağlayan bir organizasyon kültürüdür. Tehdit modellemesi, kötüye kullanılabilecek güvenlik zayıflıklarını bulmak ve vurgulamak için bir saldırganın merceğiyle uygulamalara bakmaktadır. Yazılım geliştirme yaşam döngüsü boyunca potansiyel tehditleri tespit ederek güvenlik, sonradan düşünülmek yerine öncelik hâline gelir ve güvenlik ve geliştirme ekiplerine

zaman ve para tasarrufu sağlar. Bu, güvenliğin kültürün bir parçası olmasına yardımcı olarak bir DevSecOps çalışma ortamının temelini oluşturur. Ayrıca, tehdit modelleme, ekiplerin birbirlerinin rollerini, hedeflerini ve acı noktalarını daha iyi anlamalarına ve öğrenmelerine yardımcı olur, bu da daha anlayışlı ve iş birlikçi bir organizasyon oluşturmaya imkân sağlar. Aşağıda tehdit modellemesinden kullanılabilecek bazı araçlar listelenmiştir.

- CAPEC
- IriusRisk
- Larry Osterman's Threat Modeling
- Microsoft SDL Threat Modeling Tool
- SeaSponge
- Threat Risk Modeling
- Threat Play Book
- Threat Spec

Geliştirim Adımı

Geliştirme veya geliştirim aşamasında, pek çok güvenlik denetimlerinin gerçekleştirilmesini sağlayan birçok araç ve yöntem bulunmaktadır. Bütünleşik geliştirme ortamlarının (IDE) çoğunda bütünleşik olarak gelen kod güvenlik analiz modülleri bulunmaktadır. Bunların haricinde ayrıca satılan veya açık kaynak kodlu olarak sunulan üçüncü taraf yazılım ve araç setleri de kullanılabilir.

Yazılım geliştirim esnasında aynı zamanda çapraz kod gözden geçirme faaliyetlerinin de gerçekleştirilmesine olanak tanıyan araçlardan faydalanılabilir. Bu araçlar çoğu zaman planlama aşamasında da kullanılan bütünleşik DevSecOps hattı yönetim araçları içerisinde yer almaktadır.

Yazılım geliştiriminin tamamlanması ve kaynak kod deposuna gönderilmesi ile kaynak kod deposunda da benzer şekilde statik kod güvenlik araçları ile kod analizleri yapılmalıdır. Aşağıdaki araçların pek çoğu hem IDE hem de kaynak kod deposunda statik kod analizi yapma yeteneklerine sahiptir.

- SonarQube
- Microsoft Visual Studio SDL

- Microfocus Fortify SCA
- Flawfinder
- Graudit
- RIPS
- Vault
- Snyk
- Codacy
- Veracode
- Owasp ve Npm Araçları
- Git-Secret
- Talisman
- Git Hound

Derleme ve Oluşturma Adımı

Otomatik derleme ve oluşturma araçları uygulamaların, servislerin ve kütüphanelerin uygulama paketlerine dönüştürülmesini sağlarlar. Bu aşamada derlenebilir kodlar için statik kod analizleri yapılabilir, derlenmesine gerek olmayan yazılım ve uygulamar için ise "Linter" olarak adlarılan uygulamalar ile statik kod analizleri gerçekleştirilebilir. Ayrıca bu araçlar, uygulamanızda kullanılan güvensiz kütüphaneleri tanımlamak ve yenileriyle değiştirmek için de kullanılabilirler. Burada kullanılacak olan araçlar genellikle geliştirim adımı ile benzerlikler taşımaktadır. Farklı olarak aşağıdaki araç setleri kullanılabilir:

- Chef Inspec
- Nessus
- Nexus
- Azure DevOps
- Dependency-Check
- Requires.io
- Retire.js
- Bandit
- Rips

Test Adımı

Test araçları, yazılım geliştirme yaşam döngüsü boyunca süreklilik arz eder. Test faaliyetleri, bunlarla sınırlı olmamak üzere, birim testi, fonksiyonel test, entegrasyon testi, sistem testi, regresyon testi, kabul testi, performans testi ve çeşitli güvenlik testlerini içerebilir.

Her ekip isterse kendi test kalıplarını seçebilir ve yazılımlarının ve ortamlarının ihtiyaçlarına bağlı olarak birkaç testi birleştirebilir. Tüm testler, ayrıntılı test prosedürleri, test senaryoları ve test verileri geliştiren test geliştirme ile başlar. Otomatik test, belirli bir test aracı üzerinde bir dizi test komut dosyası çalıştırılarak veya bir dizi test senaryosu çalıştırılarak insan müdahalesi olmadan yürütülebilir. İyi bir DevSecOps'ta istenilen tam otomasyon olsa da bazı durumlarda elle testlerin yürütülmesi de gerekebilir. Test adımında yapılacak testler statik veya dinamik olabilir. Aşağıdaki araçlar listesinde test adımında kullanılabilecek bazı araçlara yer verilmiştir:

- WebInspect
- Acunetix
- Contrast Security
- Sucuri
- NetSparker
- Owasp ZAP
- Checkmarx
- GauntIt
- JUnit
- TestNG
- Selenium
- SoapUI
- Microfocus Unified Functional Test
- IBM Rational Functional Tester

Sürüm Yayınlama ve Dağıtım/Teslim Adımı

Sürüm yayınlama ve teslim aşamasında, tüm derlenmiş veya paketlenmiş yazılım ve ilgili altyapı bileşenlerinin güvenlik denetimlerinin yapılmasına,

uygulamalar içerisindeki, konfigürasyonların denetlenmesine yardımcı olan araçladır.

Bir yazılımın çıktısı çok farklı ürün depolarında barındırılabilir. Aynı zamanda birden fazla dağıtım ve çalıştırma ortamı da bulunabilir. Çeşitli kapsayıcılar ile paketlenebilir. Tüm bu süreçlerde güvenliği en üst düzeyde sağlamak ve bir otomasyon içerisinde yönetebilmek için daha önceki fazlarda kullanılan araçlardan faydalanmak mümkündür. Bunların haricinde aşağıdaki araçlar da kullanılabilir:

- OpenVAS
- DockScan
- OpenSCAP
- Anchore
- Clair
- Hashicorp Vault
- Confidant
- Keywhiz
- Ansible

Operasyon ve Yayınlama Sonrası Adımı

Operasyon ve yayınlama sonrası araçları, kapsayıcılar ve sanal makina (İng. virtual machine) görüntüleri dâhil olmak üzere yazılım nesnelerini üretim ortamına yerleştirme ve sonraki çalıştırma ve işleme süreçlerini izleme olanağı sağlar. Bu adımda birçok test, izleme, güvenlik ihlal tespit ve engelleme, alt yapı yönetim ve denetleme, olay sonrası müdahale ve cevap verme, analiz araçları yer alabilir. Her bir birim ve ekip için farklı araç setleri olabileceği gibi, birbiri ile bütünleşmiş araçlar da kullanılabilir. Örnek olarak aşağıdaki araçlar verilebilir:

- AWS Cloud Formation
- Azure Automation
- Azure Resource Manager
- AWS Inspector
- AWS GuardDuty

- AWS CloudWatch
- Azure Security Center
- Azure Application Insight
- SonarQube
- Snort
- AppDynamics
- Splunk

12.7. SONUÇ VE DEĞERLENDİRMELER

Bu bölümde önce DevOps ve ardında da DevSecOps kavramları açıklanmıştır. DevSecOps süreci DevOps sürecinin güvenlik ve güvenilirlik bağlamında genişletilmesi sonucunda ortaya konmuştur. Güvenlik kavramı bilişim alanında hep sonradan eklenen bir konu olma özelliğini burada da göstermiştir. DevSecOps, uygulama geliştirme yaşam döngüsünde baştan sona kadar olan süreç ve sonrası dâhil güvenliğin benimsemesi ile olası güvenlik açıklarının her düzeyde tespit veya tahmin edilmesine ve giderilmesine imkân sağlayan bir metodolojidir. Klasik yaklaşımda her bir görev farklı rollerde yer alırken, DevSecOps tıpkı DevOps'ta olduğu gibi görevlerin birbiri içerisine geçmesine olanak tanır.

DevSecOps, riskleri ve hataları en az düzeye indirerek ve temel güvenlik sorunlarının olası en erken zamanda tespit edilmesini ve giderilmesini sağlarken aynı zamanda ciddi bir zaman ve maliyet tasarrufu getirir. Bunlara ek olarak; olay sonrası hızlı toparlanma, izleme, denetleme ve uyarı sistemleri ile anında haberdar olma ve tasarım gereği güvenliğin benimsenmesi gibi temel katkıları da bulunmaktadır.

DevSecOps insan, yönetişim, süreç ve teknoloji bileşenlerin etkin bir şekilde kurgulanması ile başarılı olabilir. Her bir bileşenin kendi içinde ve bileşenlerin birbirleri arasındaki etkileşimlerin sürekli iyileştirilmesini hedefler. DevSecOps yazılım üretim hattı üzerinde çalışır ve bu hat üzerindeki her bir aşamaya güvenliği ve güvenilirliği etkin bir şekilde ekler. DevSecOps; planlama, geliştirim, derleme ve oluşturma, test, sürüm yayınlama ve dağıtım/teslim, operasyon ve yayınlama sonrası aşamaları için çok geniş bir araç kümesine sahiptir. Bu araçlara ilişkin örnekler bölüm içinde verilmiştir.

Sonuç olarak DevSecOps yeni ancak çok hızlı gelişen bir alandır. Bulut teknolojilerindeki gelişmelere ve bu teknolojilerin kullanım yoğunluğuna bağlı olarak önemi önümüzdeki yıllarda daha da artacaktır. DevSecOps hem felsefe hem süreç olarak iyileştirmeye ve geliştirmeye açıktır. Ayrıca, hem iyi uygulama örnekleri açısından hem de araç kümesi açısından çok eksiği bulunmaktadır.

KAYNAKLAR

[1]. DevOps, https://devops.com, en son 15 Ağustos 2020 tarihinde erişilmiştir.

[2]. DevOps, https://software.af.mil/training/devops/, en son 15 Ağustos 2020 tarihinde erişilmiştir.

[3]. DevOps Model Defined, https://aws.amazon.com/devops/what-is-devops/, en son 15 Ağustos 2020 tarihinde erişilmiştir.

[4]. Understanding DevOps, https://www.redhat.com/en/topics/devops, en son 15 Ağustos 2020 tarihinde erişilmiştir.

[5]. What is DevOps?, https://azure.microsoft.com/en-us/overview/what-is-devops/, en son 15 Ağustos 2020 tarihinde erişilmiştir.

[6]. DevOps: The IT Leader's Guide, https://enterprisersproject.com/devops, en son 15 Ağustos 2020 tarihinde erişilmiştir.

[7]. CSA Security Trust Assurance and Risk (STAR), https://cloudsecurityalliance.org/star/, en son 15 Ağustos 2020 tarihinde erişilmiştir.

[8]. DevSecOps Manifesto, https://www.devsecops.org, en son 15 Ağustos 2020 tarihinde erişilmiştir.

[9]. DevSecOps Presentations, https://www.devsecops.org/presentations, en son 15 Ağustos 2020 tarihinde erişilmiştir.

[10]. What is DevSecOps?, https://www.redhat.com/en/topics/devops/what-is-devsecops, en son 15 Ağustos 2020 tarihinde erişilmiştir.

[11]. What is DevSecOps?, https://araido.io/what-is-devsecops/, en son 15 Ağustos 2020 tarihinde erişilmiştir.

[12]. DevSecOps: A Complete Guide to What, Why, and How, https://www.plutora.com/blog/devsecops-guide, en son 15 Ağustos 2020 tarihinde erişilmiştir.

[13]. DevSecOps: Embedded Security Within the Hyper Agile Speed of DevOps, https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/DevSecOps-Explained.pdf, en son 15 Ağustos 2020 tarihinde erişilmiştir.

[14]. Application Security needs a good story, https://www.acrosec.jp/strengthening-application-security-needs-a-good-story/?lang=en, en son 15 Ağustos 2020 tarihinde erişilmiştir.

[15]. Top 15 DevSecOps Tools for an Enterprise CI/CD Pipeline, https://levelup.gitconnected.com/top-15-devsecops-tools-for-an-enterprise-ci-cd-pipeline-bd865b47ed5f, en son 15 Ağustos 2020 tarihinde erişilmiştir.

[16]. What is DevSecOps? Why it's hard to do well, https://www.csoonline.com/article/3245748/what-is-devsecops-developing-more-secure-applications.html, en son 15 Ağustos 2020 tarihinde erişilmiştir.

[17]. DoD Enterprise DevSecOps Reference Design, Version 1.0, https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf?ver=2019-09-26-115824-583, en son 15 Ağustos 2020 tarihinde erişilmiştir.

Bölüm 13

ENDÜSTRİYEL KONTROL SİSTEMLERİNİN SİBER GÜVENLİĞİ

İsmail Erkek - Erdal Irmak

Son yıllarda bilişim teknolojilerinde yaşanan hızlı gelişimler, Endüstriyel Kontrol Sistemleri (EKS) ve Danışmalı Kontrol ve Veri Toplama (Supervisory Control And Data Acquisition, SCADA) sistemlerini etkileyen güvenlik zafiyetlerini de arttırmıştır. Bu nedenle bu bölümde, kritik altyapı olarak değerlendirilen EKS/SCADA sistemlerinin güvenliği üzerinde durularak bu sistemleri oluşturan bileşenler ve haberleşme protokolleri incelenmiş, bu bileşenlerin en bilinen zafiyetleri ele alınmış ve literatürde bilinen siber saldırılar analiz edilmiştir. Ayrıca endüstriyel haberleşme protokollerinin kullanım istatistikleri çıkarılarak bunlar arasında önemli yeri olan Modbus TCP protokolünün barındırdığı kimlik doğrulama zafiyetinin ve veri iletimi sırasında haberleşme olmaması zafiyetinin istismar edilebildiği, örnek bir olay takdimi olarak sunulmuştur. Bu kapsamda, Modbus TCP protokolüne dışarıdan ve içeriden müdahale edilerek SCADA bileşenleri arasında akan paketlerin manipüle edilebildiği gösterilmiştir. Sunulan çalışmanın kritik bir altyapı olan SCADA sistemlerinde siber güvenliğe yönelik farkındalığın arttırılmasına katkı sağlayacağı değerlendirilmektedir.

13.1. GİRİŞ

Günümüzde elektrik, doğalgaz, su, kanalizasyon, ulaşım, ilaç ve kimya sanayisi, kâğıt hamuru ve kâğıt sanayisi, yiyecek içecek sektörü ve parçalı üretim sanayisinde kontrolü ve izlenmesi Endüstriyel Kontrol Sistemleri (EKS) veya Danışmalı Kontrol ve Veri Toplama Sistemleri (Supervisory Control And Data Acquisition, SCADA) ile sağlanmaktadır. Bu sistemlere yönelik gerçekleştirilen fiziksel ve siber saldırılarla yetkisiz erişim elde edilebilmekte ve farklı müdahalelerle bu sistemlerin işleyişi ve fonksiyonu değiştirilebilmekte ve bozulabilmektedir.

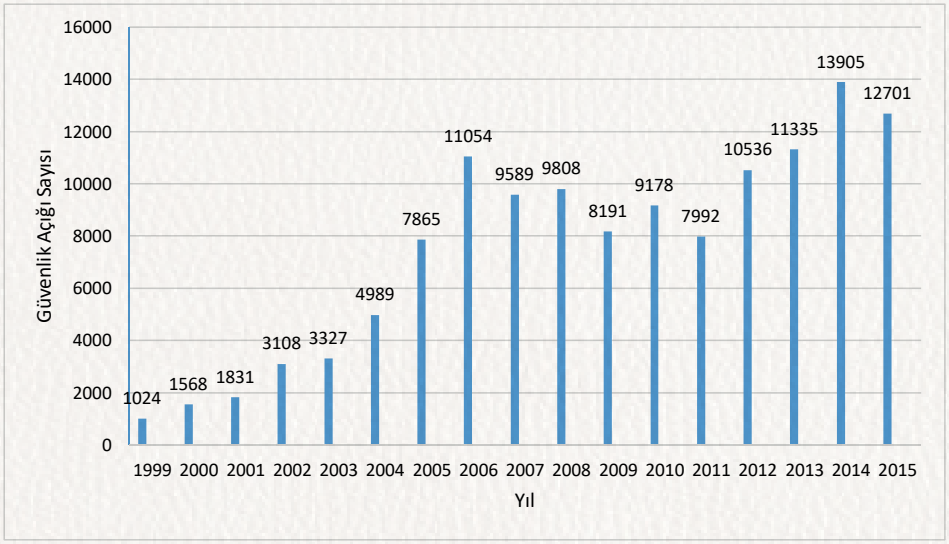
EKS bağımsız bir birim olarak işlenecek şekilde tasarlanmasına rağmen kurumsal bir ortamda çalışır. Kontrol sistemi tasarımının en önemli amacı verimlilik ve güvenliktir. EKS'de görülen bir diğer durum rutin olarak bakım işlemlerini gerçekleştirmek için uzaktan erişim sağlamaktır. EKS haberleşme protokolleri tasarlanırken güvenlik özellikleri geri planda tutulmuştur. Kritik altyapılardaki bu gibi güvenlik açıkları kritik altyapıları siber saldırılara karşı daha hassas duruma getirmiştir. Saldırganlar, saldırılarını bu güvenlik açıklarını sömürerek gerçekleştirir. Bu saldırıların etkileri ve sonuçlarına aşağıda değinilmiştir [1]:

- Fiziksel etki: SCADA sisteminin işlevsiz kalmasının sonuçları bu alanda değerlendirilir. Bu etkinin en önemli sonucu insan hayatını tehlikeye atacak sonuçlarının olmasıdır. Diğer sonuçlarında veri kaybı ve çevreye olan zararlarıdır.
- Ekonomik etkileri: Ekonomik etkiler siber saldırıdan sonra ortaya çıkar. Fiziksel etkinin dalgalanma etkisi tesis veya firmada ciddi ekonomik kayıpları beraberinde getirir. Daha büyük etkisi yerel, ulusal hatta küresel ekonomi üzerinde ekonomik kayıplara neden olmasıdır.
- Sosyal etkileri: Fiziksel ve ekonomik hasarların sonucu kamu güveni ve ulusal güvenliğin zarar görmesi olacaktır. Sosyal etkiler kamu güvenliğini depresif bir hâle getirebilir ya da popüler aşırılığın artmasına sebep olabilir.

Yaygın olarak görülen güvenlik tehditleri ve saldırılarında ortaya çıkan sonuçların büyüklüğünden dolayı daha güvenli bir SCADA sistemi geliştirmek

amacıyla çeşitli kurum ve kuruluşlar SCADA sistemlerine yönelik saldırılara karşı kapsamlı çalışma ve araştırmalar yapmaktadır.

Literatürde SCADA sistemlerinde tespit edilen güvenlik açıklarının en güncel istatistiği Şekil 13.1 verilmiş olup bilgi sistemlerinde oluşan güvenlik açıklarının ciddi oranda artış gösterdiği anlaşılmaktadır. 1999 – 2016 yılları arasında tespit edilen güvenlik açıklarında yaklaşık 12 kat büyüme olduğu fark edilmiştir. Bilgi teknolojileriyle entegre çalışan SCADA sistemleri de direk olarak bu tehditten etkilenmektedir.



Şekil 13.1. Yıllar bazında güvenlik açığındaki değişim [2]

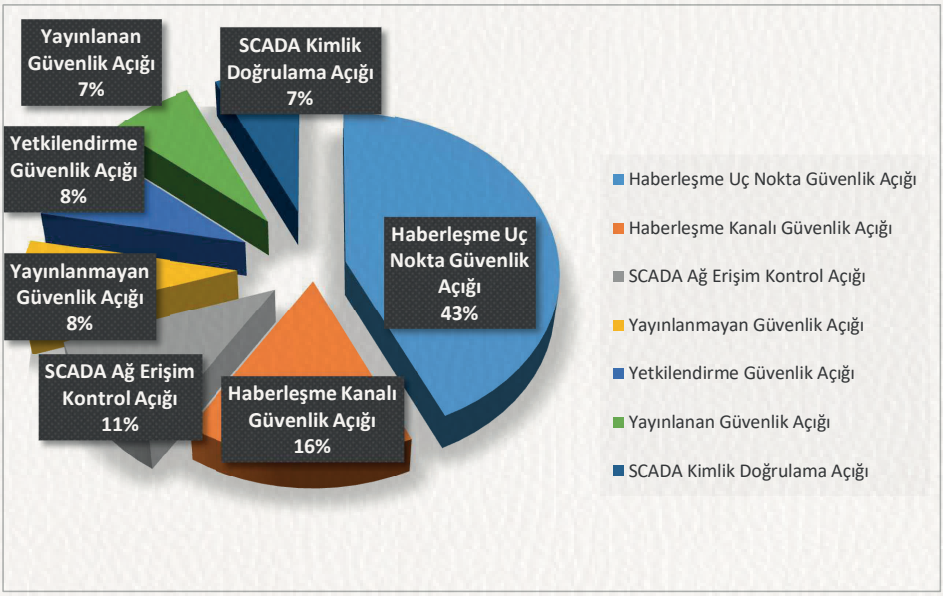
SCADA sistemleriyle ilgili "SCADA sistemleri fiziksel olarak birbirinden ayrı ve bağımsızdır" düşüncesi genel bir yanlış düşüncedir. Birçok SCADA sistemi ağ bileşenlerinden önce yapılmış ve ağın geri kalanından ayrı tasarlanmıştır, bu durum sistem yöneticilerini diğer kurumsal ağlardan veya erişim noktalarından bu sistemlere erişim olamayacağı düşüncesine inandırmıştır. Maalesef bu düşünce tamamen yanlıştır. Gerçek senaryoda SCADA ağı ve kurumsal ağlar bilgi yönetiminde oluşan değişikliklerden dolayı köprülüdür. Bu değişikliklerde önemli rol oynayanlar aşağıda açıklanmıştır [3]:

- İlk değişiklik, kurumsal ağda erişim noktasından sistemi uzaktan izleme ve denetleme için SCADA mühendislerine sisteme bağlantı kurmasına olanak sağlayan artan taleptir.
- İkinci temel sebebi kurumsal bir karara yardımcı olmak amacıyla bilgi erişimidir. Birçok kamu kurumunun kritik bilgilere ve işlevsel durumu daha yüksek bir yönetim için veya kurumsal karar almak için ani erişim yapması gibi SCADA sistemlerine kurumsal bağlantı izni vardır.

SCADA sistemleriyle ilgili bir diğer büyük yanlış düşünce; "SCADA sistemleri ve diğer kurumsal ağlar arasındaki bağlantı güçlü bir erişim kontrolüyle korunur"dur. Kurumsal ağ ve SCADA sistemleri arasındaki birçok bağlantı, farklı bağlantı standartları ile sistem entegrasyonuna ihtiyaç duyar. Ağ yöneticilerinin ağ erişim anahtarlarını göz ardı etmesi nedeniyle kurumsal ağlar üzerinden yetkisiz erişim SCADA sistemi koruması için tasarlanan erişim kontrolü genelde asgari düzeydedir. Güvenlik duvarları ve saldırı tespit sistemlerinin (STS) güçlü parola koruması ile kullanımı tavsiye edilir.

13.2. SCADA SİSTEMİ GÜVENLİK AÇIKLARI

Idaho Ulusal Laboratuvarı'nın (INL) ABD Enerji Bakanlığı Elektrik Dağıtımı ve Enerji Güvenliği Dairesi'ne sunduğu raporda [4] Ulusal SCADA Test Düzeneği (NSTB) programıyla ulusal enerji altyapısının siber saldırılar karşısında güvenliğinin ve esnekliğinin sağlanması hedeflenmiştir. Bu programın temel amacı SCADA sistemlerindeki güvenlik açıklarını analiz ederek saldırı etkisini hafifletme yaklaşımlarını tanımlayıp saldırılara karşı önlem almaktır. Raporda SCADA sistemine yönelik gerçekleştirilen siber saldırılarda istismar edilen güvenlik açıkları sınıflandırılmış ve analiz edilmiştir. İlgili raporun 2011 yılında yayımlanmış olmasına rağmen, içerdiği bilgiler ve elde edilen sonuçlar literatürdeki SCADA sistemlerinin siber güvenliği ile ilgili teknik çalışmalar içerisinde en kapsamlı olmasından ötürü bu tez çalışmasında ilgili yerlerde bu rapordan faydalanılmıştır. Şekil 13.2'de NSTB'e göre gözlemlenen güvenlik açıklarının çeşitlerine göre yüzdeleri verilmiştir.



Şekil 13.2. NSTB SCADA güvenlik açığı sıklığı [4]

Şekil 13.2'de gösterilen güvenlik açıklarından birçoğu bellek taşması (buffer overflow)'dır. Örneğin gösterilen bir uygulamada 50 saldırı vektöründen 50'sinde bellek taşması tespit edilmiş ve bunların hepsi tek bir güvenlik açığı olarak hesaplanmıştır. Tek bir kimlik doğrulama atlatma tekniği de bir güvenlik açığı olarak hesaplanmıştır. SCADA sistemlerinde tek bir güvenlik açığı diğer sistemlere oranla çok daha fazla kritik veya geniş kapsamlı olabilir. Örneğin, bir SCADA protokolündeki bir haberleşme kanalının güvenlik açığı tüm sistemi etkileyebilmekte ve bu bir zafiyet olarak sayılmaktadır. Değerlendirme ekibinin ve SCADA üreticilerinin deneyimiyle belirlenen NSTB değerlendirmeleri SCADA sistemini ele geçirme olasılığı ve etkisi bazında değerlendirme hedeflerine (Kontrol sistemi üzerinde ciddi etkilere sebep olan giriş noktası, işlemler, protokoller vb.) öncelik verilmiştir. Tablo 13.1'de SCADA güvenlik açığı tipleri ve temel SCADA fonksiyonlarına erişebilen ilgili değerlendirme hedefleri açıklanmıştır.

Tablo 13.1. Temel SCADA fonksiyonlarına erişebilen açıklıklar ve ilgili değerlendirme hedefleri [4]

Güvenlik Açığı Tipi	Değerlendirme Hedefi Kategorisi	Güvenlik Açığı Kaynağı
Bilinen Güvenlik Açıkları	En Muhtemel Saldırı Yolları	SCADA ürünlerine eklenmiş eski veya yamasız üçüncü parti uygulamaları
		SCADA Sunucuları üzerinde koşan yamasız İşletim Sistemleri
Yayınlanmayan Güvenlik Açıkları	Potansiyel 0-gün veya Yamalanmamış Güvenlik Açıkları	Gereksiz Servisler üzerinden SCADA Sunucusunu açıkta bırakma
		Hatalı SCADA Kodu
Haberleşme Kanalı Güvenlik Açıkları	Güvenlik Açığı olan Haberleşme Kanalı üzerinden SCADA İşlevselliğine Yetkisiz Erişim	Spoofing ve araya girme saldırılarına karşı zafiyet barındıran uzaktan erişim protokolleri
Haberleşme Son Nokta Güvenlik Açıkları	SCADA Sunucularına veya Uygulamalarına Yetkisiz Erişim veya DoS	SCADA Haberleşmesi ve veri transferi protokolleri için zafiyet barındıran Sunucu Uygulamaları
		Veri Tabanı Güvenlik Açıkları
		Web Güvenlik Açıkları
SCADA Uygulama, Kimlik Doğrulama Açıkları	Kimlik Doğrulama Mekanizmasını İstismar ederek SCADA Uygulamalarına Erişim	Kimlik Doğrulama Atlatma
		Kimlik Bilgileri Yönetimi
SCADA Sunucu Yetkilendirme Açıkları	SCADA Hesabından Sisteme Zarar verebilme	Sunucu yapılandırma güvenliğinde yapılan hata
SCADA Ağı Güvenlik Açıkları	Uygun Ağ Yolları üzerinden SCADA Sunucularına ve İşlevselliğine Erişim	Hatalı Ağ Tasarımı
		Zayıf Güvenlik Duvarı Kuralları
		Ağ Cihazı Yapılandırma Hataları
		Hatalı Ağ İzleme

NSTB değerlendirmesinin sonuçlarına göre SCADA fonksiyonlarını riske atan ve haberleşmesini engelleyebilen veya aksatabilen SCADA sunucularına, uygulamalarına veya verilerine yetkisiz erişim sağlayabilen güvenlik açıkları tanımlanıp analiz edilmiştir. Bu güvenlik açıkları aşağıdaki gibi açıklanmıştır.

13.2.1. Kaynak Kodu Tasarımı ve Uygulaması

SCADA uygulamaları ve servislerindeki güvenlik açıklarını minimize etmek için güvenli kodlama yapılması gerekmektedir. Yazılımda oluşabilecek güvenlik açıkları kötücül amaçlar için istismar edilip SCADA sistemini saldırılara açık hâle getirebilir, bu yüzden sistem yöneticileri ilk yapılandırmadan sonra yapacakları değişikliklerde tereddüt içinde olabilirler [5].

SCADA yazılım incelemeleri ve tersine mühendislik çalışmaları SCADA yazılımının her zaman güvenli bir konseptte yapılmadığını göstermektedir. NSTB değerlendirmelerinde gözlemlenen SCADA yazılım açıklarının güvensiz yazılım ve yeterli olmayan testler sonucunda oluştuğu ortaya çıkmıştır. Gözlemlenen en önemli üç açıklık; girdi doğrulaması, kimlik doğrulama ve erişim kontrolüdür. NSTB değerlendirmelerinde ortaya çıkan güvenlik açıklarının birçoğunda tehlikeli fonksiyonlara sebep olan uzaktan kod çalıştırılabilmektedir. SCADA yazılımları büyük, karmaşık ve eski kod tabanlı olabilirler ve SCADA işlemleri yüksek kullanılabilirliğe ihtiyaç duyabilir ve güncelleme senaryoları karmaşık olabilir. Kullanıma hazır bilgisayar yazılım modeli standartlarının aksine güvenlik düzeltme maliyeti, desteği ve bakımı SCADA kullanıcısına geleneksel olarak transfer olmuştur. SCADA ürün açıklarının yayınlanması SCADA güvenliği için yeni bir gereklilik ile SCADA üreticileri kod denetimi ve ilgili kod değişikliklerini bulabilirler. Güvenli kod kaynakları tüm uygulama türleri ve dilleri için bulunabilir. CWE (Common Weakness Enumeration) listesi [6] bilinen birçok SCADA programlama hatalarının dâhil olduğu tüm yazılım açıkları hakkındaki bilgiler Tablo 13.2'de verilmiştir.

Tablo 13.2. Güvenli olmayan SCADA kod tasarımı ve uygulamasıyla ilgili bilinen açıklıklar [7]

Açıklık Sınıflandırması	Bilinen Açıklıklar
CWE-19: Veri İşleme	CWE-228: Sözdizimsel geçersiz yapının hatalı işlenmesi
	CWE-229: Değerlerin hatalı işlenmesi
	CWE-20: Hatalı girdi doğrulama
	CWE-116: Hatalı kodlama
	CWE-198: Hatalı bayt sıralaması kullanımı
CWE-119: Bellek sınırı içinde sınırlama işlemi hatası	CWE-120: Giriş boyutu kontrolü olmadan bellek kopyalama (Klasik bellek taşırma)
	CWE-121: Stack-based (yığın tabanlı) bellek taşırma
	CWE-129: Dizi indeksini hatalı doğrulama
	CWE-190: Integer taşırma veya silme
	CWE-680: Integer veya bellek taşırma
CWE-398: Kötü kod kalitesi göstergesi	CWE-454:Güvenilir değişkenlerin veya verilerin dışarıdan başlatılması
	CWE-456: Eksik başlatma
	CWE-400: Kontrolsüz kaynak tüketimi
	CWE-252: Denetlenmeyen dönüş değeri
	CWE-772: Eksik kaynak yayınlanması
CWE-442: Web Problemleri	CWE-22: Kısıtlı bir dizine hatalı yol adı limitlemesi (Yol Geçişi)
	CWE-79: Web sayfası koruma alanı hatası (XSS)
	CWE-89: SQL sorgu yapısı koruma alanı hatası (SQL enjeksiyonu)

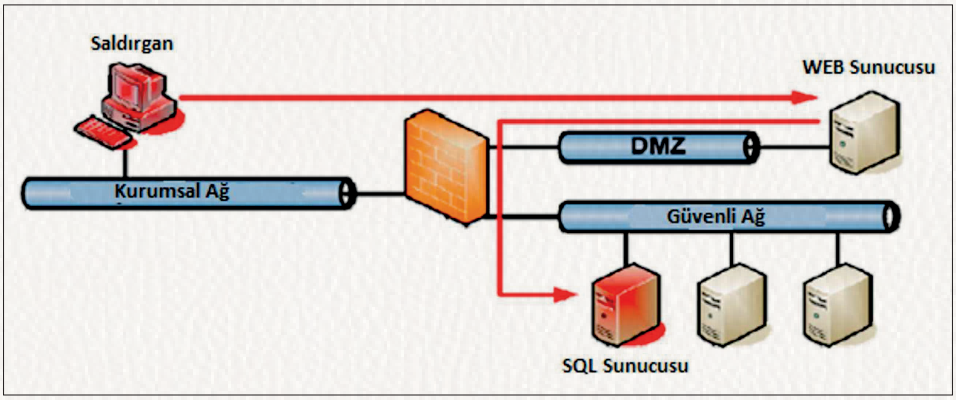
13.2.2. Bellek Taşırma (Buffer Overflow)

Bellek taşırma açığı SCADA sistemlerinde en sık karşılaşılan girdi doğrulama zayıflığından kaynaklanmaktadır. Bellek taşırmalar yazılımın belleğe hafızada ayrılan boşluktan daha fazla veri yazılmasıyla oluşmaktadır. “Extra” veri, bitişik belleğin üzerine yazılır ve programın normal fonksiyonları dışında çalışmasına sebep olur. Dikkatlice planlanmış ve çalıştırılmış bellek yazma, programın saldırgan tarafından çalıştırabilmesine sebep olur. İstismar kodu

interaktif bir oturum oluşturmak ve istismar edilmiş programın yetkileriyle kötücül komut göndermek için bellek taşmasını kullanır. Bellek taşırma, ağ trafiği sürecindeki uygulamalarda, veri transferi sırasında girdi değerlerinin durdurulup değiştirilerek istismar edilmesiyle gerçekleştirilir. Sonuç olarak, girdi değerlerinin doğrulamasının olmadığı ağ protokolü uygulamaları bellek taşırma saldırılarına karşı savunmasızdır [8]. Örneğin geliştirici, hiç kimsenin kullanıcı adı olarak 1024 karakterden daha uzun karakter yaratmayacağını düşünebilir. Geliştirici, kullanıcı adı için belleğe 1024 baytlık bir alan oluşturur ve girdi doğrulaması yapmazsa, bir saldırgan, 1024 karakterden daha fazlasını keşfetmek için birçok kullanıcı adını deneyebilir. Geliştirici, girdi alanında depolanan bellek için ayrılan boyutu aşmayacak şekilde girdi boyutunda doğrulama yaparak bu açığı kapatabilir.

13.2.3. SQL Enjeksiyonu

SQL sorgu komutunda kullanılan özel karakterlerin bütünlüğünü garanti etmeyen kullanıcı girdilerinin hatalı veya yetersiz filtrelemesi sonucu oluşan SQL enjeksiyonu açığı SCADA geçmiş (historian) veri tabanına etki edebilir. Mesela, bir saldırgan bir veri tabanı sorgusuna hazır bilgi çıkış karakteri eklerse, saldırgan veri tabanına rasgele okuma/yazma erişimi sağlayabilir. SQL komutu veri tabanıyla haberleşmek için kullanılır. Aynı zamanda SQL sorguları kimlik doğrulama gibi güvenlik kontrolleri için kullanılabilir, saldırganlar güvenliği aşmak için bu sorgulardaki mantıklarda değişiklik yapabilir [9]. SQL enjeksiyonu açıkları istemci (genelde Web) uygulamaları üzerinde bulunur. SQL enjeksiyonu SQL komutlarını veri tabanına yönlendirerek veri tabanını istismar eder. Veri tabanı destekli uygulamalar güvenli ağ üzerinde sunucudan veri alabiliyorsa SQL enjeksiyon için bir hedeftir. Örneğin, bir istemci uygulaması Şekil 13.3'te gösterildiği gibi arındırılmış bölge anlamına gelen ve dış ağlara açık servislerini içeren ve bu servisleri daha büyük güvensiz bir ağa (genellikle internet) maruz bırakan fiziksel veya mantıksal bir alt ağ olan DMZ'da yalıtılmış Web sunucusu üzerinden güvenli ağda veri tabanına bağlanırsa, SQL enjeksiyonu saldırıları SQL sunucusuna güvenli ağ üzerinden yapılabilir. Hatta güvenlik duvarı sunucuya olan diğer tüm bağlantıları engellese bile başarılı bir saldırı, saldırgana güvenli ağ üzerinden SQL sunucusunu kontrol etme olanağı sağlar.



Şekil 13.3. Web uygulamaları üzerinden SQL enjeksiyonu saldırısı

13.2.4. XSS (Cross Site Scripting) Açığı

XSS açıklığının temel sebebi SQL enjeksiyonunda olduğu gibi girdi doğrulama eksikliğinden kaynaklanmaktadır. Fakat, XSS saldırılarında web uygulaması kötücül kodu kullanıcıya gönderir. 2010 CWE/SANS En Tehlikeli 25 Programlama Hatası raporunda [10] XSS en sık kullanılan ve kritik programlama hatası olarak yayımlanmıştır. Saldırgana güvenlik açığı olan web uygulaması ile oluşturulan web sayfasına kod yerleştirmeye olanak sağladığı için oldukça tehlikelidir. Saldırı kodu web sunucusu yetkisiyle kullanıcı tarafında çalıştırılır.

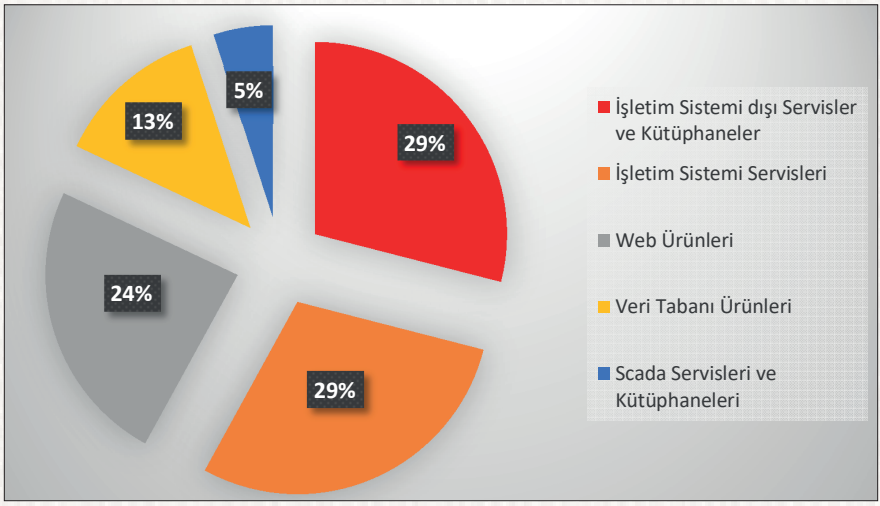
13.2.5. Gereksiz Portlar ve Servisler

Sistem üzerinde koşan servisler ve uygulamalar dış dünyayla haberleşmek için bazı ağ portlarını açabilir. Bir saldırgan açık port üzerinden SCADA sistemine erişim sağlayıp sistem hakkında bilgi toplayabilir. Her açık port saldırgana istismar kodunu göndermeye ve veri çekmesine olanak sağlayabilir. Saldırgan erişilebilir ağ portlarını dinleyen servislere uzaktan bağlantı kurarsa, hedef ağ üzerinde kendisine yer bulabilir ve yerel ağ sunucularını dinleyen tüm servisleri hedef alabilir. Güvenlik açığı olan ağ uygulaması, saldırgan tarafından istismar edilebilir ve yetkisiz bir şekilde verileri çekmek için kötücül kod göndermesine sebebiyet verebilir [11]. SCADA sunucuları üzerinde ne kadar çok çalışan servis varsa SCADA sisteminin saldırıya maruz kalma-

sı o kadar potansiyel dâhilindedir. Sonuç olarak, SCADA sistemi üzerinde mümkün olduğunca gerekli servis ve uygulamalar çalıştırılmalıdır, böylece kullanılmayan portlar kapalı olacaktır.

13.2.6. Etkili Yama Yönetimi Uygulaması

İşletim sistemi, servisler, kullanıcılar ve üçüncü parti yazılımlar için etkili yama yönetimi çok önemlidir. SCADA üreticileri ürünlerinde kullanıcılarına yamaları uygulayarak güvenlik açıklarını hafifletebilirler. Hafifletme uygulanmadan önce güvenlik açıklarının hızlıca tanımlanması ve yamalarının yapılması açıklığın ifşasının riskini minimize eder. Aynı zamanda SCADA üreticileri yamalarını üçüncü parti ürünler üzerinde test eder ve daha sonra temel ürüne yamalar.



Şekil 13.4. SCADA sisteminde yamasız bileşenlerin yüzdeleri [4]

İşletim sistemi yamaları saldırganın işletim sistemi üzerinde kod çalıştırmasına olanak sağlayan güvenlik açıklarını kapatmak için yayımlanır. 2009 Siber Güvenlik Risk Raporu'na göre [12], son yıllarda uygulamalarda keşfedilen güvenlik açıkları işletim sistemlerinde keşfedilen güvenlik açıklarından çok daha fazladır. Sonuç olarak uygulama programlarında kaydedilen saldırı girişimi daha fazladır. Şekil 13.4'te NSTB değerlendirmesinde SCADA sisteminde yamasız yazılım bulunan ürünlerin yüzdeleri verilmiştir.

13.2.7. Haberleşme Kanalı Güvenlik Açıkları

SCADA sistemleri, firmaların intranetleriyle ve dış ağda internetle olan bağlantılarının artmasından dolayı siber saldırılara daha fazla maruz kalmaktadırlar. Haberleşme kanalları bu bakımdan önemlidir çünkü farklı güvenlik alanlarıyla bağlantı kurarlar, erişim yetkilerine sahip olurlar ve SCADA sistemini manipüle etmek amacıyla fonksiyonlarında değişiklikler yapılabilir. Haberleşme kanalı açıkları için aşağıdaki konular incelenmiştir:

- SCADA kimlik bilgileri toplama,
- SCADA veri ve komut aldatmacası ve manipülasyonu,
- SCADA fonksiyonlarını riske atan haberleşmelere DoS.

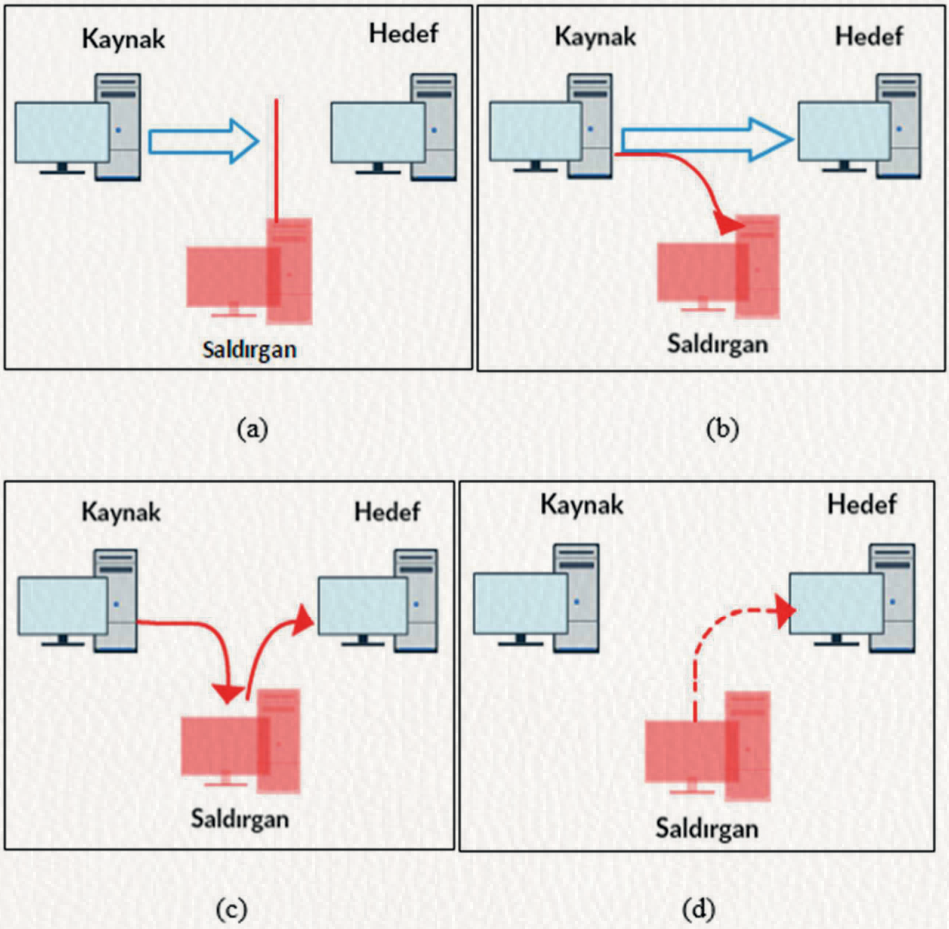
SCADA sistemlerinde; ağ cihaz yönetimi, uzaktan erişim veya dosya transferi gibi normal BT fonksiyonlarında bulunan BT protokolleri kullanılmaktadır. Bu protokollere yönelik tehditler SCADA sistemleri için de geçerlidir. Örneğin; ssh, ftp, telnet ve rlogin protokolleri gibi dosya transferi ve uzaktan erişim protokolleri SCADA sistemi ağlarında da kullanılabilmektedir. Bu protokollerden güvenli olanların tercih edilmesi önemli olmaktadır. Örneğin, haberleşme protokolleri ssh üzerinden tünellenebilir veya http, ssl üzerinden gönderilebilir (https) [13].

13.2.8. Haberleşme Protokollerinin Açıklıkları

Bu alt başlık altında SCADA haberleşme protokollerinden DNP3, Modbus TCP ve Profinet protokollerine yönelik zafiyetler ve saldırılar anlatılmıştır.

13.2.8.1. DNP3 Açıklıkları ve Saldırıları

DNP3 protokolüne yönelik saldırılar; protokolün özelliklerini, üretici uygulamalarını veya altyapısındaki zayıflıklarını istismar ederek gerçekleştirilir. Üretici uygulamalarına yapılan saldırılar, sistemde yapılandırma hatalarının istismarı şeklinde olur. Altyapı saldırıları, politika ve platformlardaki açıklıklar istismar edilerek gerçekleştirilir. Protokol özelliklerine yönelik gerçekleştirilen saldırılar daha çok haberleşme mimarisi ve DNP3 yapısıyla ilgilidir. Saldırılar yoğunlukla MTU, RTU ve haberleşme yolu olmak üzere üç hedefe yönelik gerçekleştirilmektedir. Dolayısıyla saldırılar Şekil 13.5'te gösterildiği gibi hedefe giden trafiği keserek, yakalayarak, değiştirerek ve yeniden üreterek gerçekleştirilir.



Şekil 13.5. DNP3 Saldırıları (a) Kesme (b) Yakalama (c) Değiştirme (d) Yeniden üretme

13.2.8.2. Modbus Açıklıkları ve Saldırıları

Modbus sistemlerine ve ağlarına yönelik saldırılar bu protokolün özelliklerine, uygulamalarına ve altyapısına göre istismar edilir. DNP3'teki gibi bu protokole yönelik tehditler kesme, yakalama, değiştirme ve yeniden üretme olmak üzere dört kategoride incelenebilir. Modbus Seri Protokolü'ne yapılan saldırılar ana ve köle cihazlarına ve seri haberleşme ağına yönelik gerçekleşirken, Modbus TCP'e yapılan saldırılar IP ağına, ana ve köle cihazlarına gerçekleştirilir [14].

Bu saldırılarda mesajın içeriğine erişilebilmesinden dolayı taşınan bilginin gizliliğinin ifşa olmasına sebep olunabilir, hizmet engellemesine sebep olduğu için sistem erişilebilirliğine etki eder ve araya girerek ele geçirilen bilginin yeniden üretilebilmesinden dolayı veri bütünlüğü etkilenir. Saldırılar; Modbus Seri Protokolü, Modbus TCP Protokolü ve her iki seri ve TCP Protokolleri olmak üzere üç başlık altında incelenir.

Irmak ve Erkek; yaptıkları çalışmada [15], Endüstriyel Kontrol Sistemleri'nde en sık kullanılan Modbus TCP Protokolü'nün haberleşme altyapısını incelemiş, kimlik doğrulama zafiyetinin istismarı yapılarak bu protokoldeki verilerin gizliliğinin ve bütünlüğünün bozulabildiğini tespit etmişlerdir. Bu güvenlik sorunun engellenmesine veya hafifletilmesine yönelik bir güvenlik çözüm önerisinde bulunmuşlardır.

13.2.8.3. Profinet Açıklıkları ve Saldırıları

ISO-TSAP (Standards Organization Transport Access Point) gibi endüstriyel sistemlerde kullanılan protokoller geliştirildiği dönemin şartlarındaki güvenlik konseptine göre oluşturulmuştur. Kontrol sistemlerinin ve PLC cihazlarının o dönemde tamamen izole olduğu düşünüldüğünden bu protokoller güvenli olarak tasarlanmamıştır.

Simatic S7 istismarı direk olarak Profinet'e yönelik değildir fakat Profinet istismar edilecek ağa bağlanmak için kullanılmaktadır. Saldırı, Siemens tarafından üretilen bütün S7 PLC'lerin haberleşmesi ve programlanması için Siemens mühendislik yazılımı olan ISO-TSAP'ten faydalanır.

Saldırganın bakış açısından S7 PLC cihazı ISO-TSAP ile 102. porttan haberleşmekte ve iletilen paketler açık metin olarak şifrelenmeden gönderilmektedir. Bu yüzden araya girme ve yeniden yönlendirme saldırıları bu sistem için uygun olmaktadır. Aynı zamanda MTU ve RTU veya PLC cihaz arasında akan bütün trafik kolay bir şekilde yakalanabilmekte ve böylece saldırganın protokole yönelik tersine mühendislik gerçekleştirmesine ve kötücül amaçları için kendi paketlerini üretmesine imkân sağlamaktadır.

ISO-TSAP'in bir diğer önemli güvenlik açığı, kimlik doğrulamasının zayıf olmasıdır. Kimlik doğrulaması yapılmış paketleri yakalayan bir saldırgan, aynı paketi kullanarak kimlik doğrulama mekanizmasını aşabilir [16].

Kullanıcı kimlik doğrulama paketini PLC cihazına gönderdiğinde, paketteki parola veya parola özeti cihazdaki yapılandırılmış olan parola özetiyle karşılaştırır. Eğer bu karşılaştırma doğruysa cihaz erişime izin verir ve PLC hafızasına okuma/yazma/çalıştırma yetkilerini verir. Bu, saldırganın PLC üzerinde istediği değişiklikleri yapabileceği anlamına gelmektedir.

Irmak ve Erkek; yaptıkları çalışmada [17], Profinet Protokolü'nün haberleşme altyapısı ve güvenliğini analiz edebilmek için bir deney düzeneği ortamı tasarlamışlardır. Tasarladıkları deney düzeneği ortamında araya girme (Man-in-the-middle), hizmet engelleme (Denial of Service) ve yeniden yönlendirme (Replay) saldırıları gerçekleştirerek endüstriyel cihazların tepkilerini ve haberleşme protokolünün güvenliğini analiz etmişlerdir.

13.3. SCADA GÜVENLİK TESTİ ARAÇLARI

Bilgi ve iletişim teknolojileri altyapısıyla entegre bir şekilde çalışan SCADA sistemlerinin güvenlik açıklarının tespiti ve tespit edilen bu zafiyetlerin istismarı, normal bilgi teknolojileri altyapısını kullanan sistemler için yapılan sızma testi araçları veya özel olarak SCADA sistemleri için tasarlanmış araçlar kullanılarak yapılmaktadır.

Çalışmanın bu bölümünde SCADA sistemlerinde kullanılan güvenlik testi araçların bir kısmı gösterilmiştir.

13.3.1. Shodan Arama Motoru

2009 yılında John Matherly isimli bir programcı, internet bağlantılı cihazları tanımlayabilen ve grafiksel ara yüzlü Shodan isimli bir arama motoru yazmıştır [18]. Özellikle; bilgisayar, yazıcı, webcam ve endüstriyel kontrol cihazları gibi yönlendirilebilen IP adresli cihazları tanımlayabilir. Shodan; bütün interneti tarar, cihazları dizinler ve uygun olan servislere sorguda bulunur. Shodan API veya https://www.shodan.io/ üzerinden erişilebilecek aranabilir veri tabanında topladığı cihazların IP adreslerinin port numaralarını ve üzerinde çalışan servislerin ana başlık bilgilerini barındırır. Kullanıcılar; ülke, sunucu adı, belirli IP adresi aralığı, işletim sistemi, cihaz markası veya port bilgilerini barındıran farklı sorgulamalarda bulunabilirler.

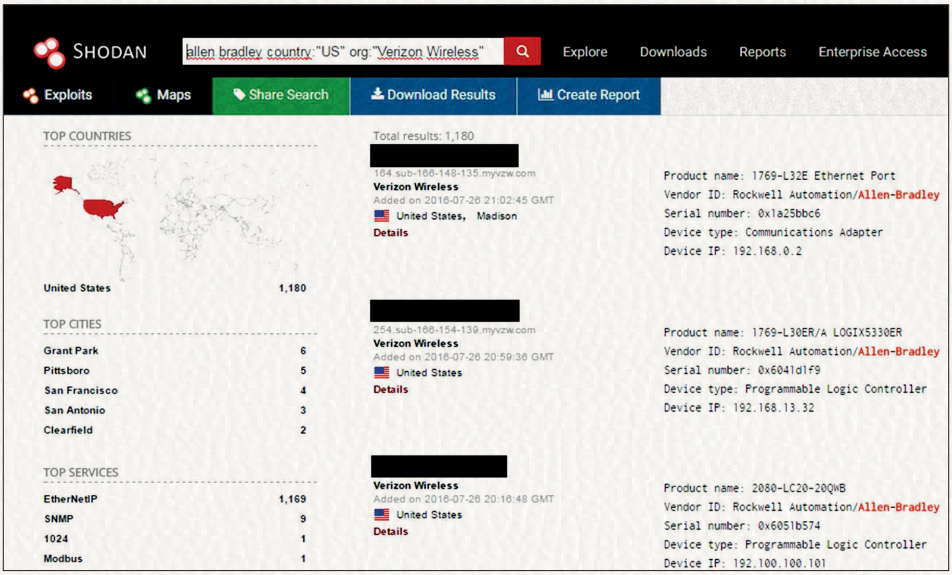
2010 yılının Ekim ayında; ICS-CERT, Shodan'ın kontrol sistemleri ara yüzlerine ait güvenlik açıklarını tespit edebilme yeteneğini ve kontrol sistemi cihazlarının internetten izole olmasının öneminin tartışıldığı bir rapor yayımlamıştır [103]. Bu raporun sonucunda ICS-CERT-10-301-01, ICS-CERT-301-01A, ICS-CERT-11-343-01A, ICS-CERT-12-046-01 ve ICS-CERT-12-046-01A olmak üzere 5 tane internetle bağlantılı kontrol sistemleri cihazlarının önemiyle ilgili rapor yayımlamıştır [19].

2011 yılında Leverett [20], 7500'den fazla internete bağlı yönetim sistemleri, sayaç, HMI ve PLC gibi endüstriyel kontrol cihazlarını kullanmıştır. Toplam 29 Shodan sorgusu endüstriyel kontrol cihazlarının tespiti için kullanılmıştır. 2 yıllık bir değerlendirme sonucunda 2013 yılında tespit edilen 7500 cihaz dramatik olarak artmış ve 57409 adet olduğu tespit edilmiştir.

2012 yılında SHINE (Shodan Intelligence Extraction) projesi A.B.D. İç Güvenlik Bakanlığında yürütülen bir proje olup [21], bu proje kapsamında Shodan API kullanılmış ve yaklaşık olarak 700 farklı Shodan sorgusuyla dünya genelinde internete bağlı 500000 adet endüstriyel kontrol cihazı tespit edilmiştir. ICS-CERT ile birlikte 7200 cihaz üzerinde yürütülen projenin devamında çoğu cihazda çok zayıf güvenlik önlemleri alındığı görülmüştür [22].

Shodan web ara yüzü kullanılarak "allen bradley" markalı internet bağlantılı endüstriyel kontrol sistemi sorgulanmış ve elde edilen sonuçlardan sistem üzerindeki zafiyetler tespit edilmiştir. Yapılan sorgulamada cihazın bulunduğu ülke ve şehirler, üzerinde çalışan servis ve portlar, işletim sistemi, markası, üzerinde çalıştığı firma adı ve IP adresi aralığı aranabilmektedir. Şekil 13.6'da yapılan sorgulamaya ait ekran görüntüsü görülmektedir.

Tespit edilen endüstriyel kontrol sistemlerine girince harita üzerinde sistemin nerede olduğu, üzerinde çalışan servisler ve portlar, cihazın ürün ismi, üreticinin markası, cihazın seri numarası, cihazın tipi ve cihazın yerel IP adresi görülmektedir. Sorgulanan cihazlardan birçoğunda web servisinin çalıştığı fark edilmiş ve bu cihazların web giriş ara yüzü ekranlarına erişim yapılabildiği ve erişim sağlanan uygulama üzerinde şifreleme yapılmadan giriş yapılabildiği tespit edilmiştir. Böylece trafiği dinleyen bir saldırgan, kullanıcının girdiği verileri şifresiz olarak görüntüleyebilmektedir.



Şekil 13.6. Shodan sorgu sonucu

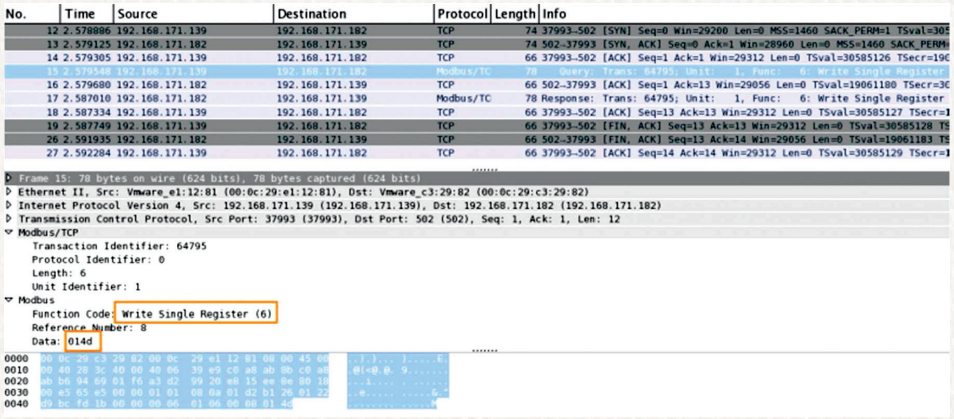
Parola güvenliğinin önemini göstermek amacıyla web servisi üzerinden giriş yapılabilen bir endüstriyel kontrol sistemine giriş yapılırken kullanıcı bilgilerinin sistem yöneticisi veya kullanıcısı tarafından değiştirilip değiştirilmediği kontrol edilmiş ve elde edilen sonuçlara göre birçok sistemde kullanıcı bilgilerinin varsayılan olarak bırakıldığı gözlemlenmiştir. Cihazların türüne göre internette yapılan varsayılan kullanıcı adları ve parolaları arandığında çok kolay bir şekilde bulunabildiği ve sisteme basit ve yetkisiz bir şekilde erişilebildiği tespit edilmiştir.

13.3.2. Wireshark Ağ Analiz Programı

Wireshark ihtiyaç doğrultusunda ağ üzerinde akan paketleri detaylı bir şekilde görüntülemeye yarayan açık kaynak kodlu bir paket analizi programıdır [23]. Ağ üzerinde akan paketleri yakalar, parçalara ayırıp inceleyerek analiz eder ve analiz ettiği protokole bağlı olarak paketteki "1'ler ve 0'lar"ı yorumlar. Ağ kullanım hesaplamaları gibi farklı istatistiksel analizlere Wireshark'ta parçalara ayrılmış paketlerdeki bilgileri kullanılarak erişilebilir. Bu sayede ağ üzerindeki cihazların birbirleri ile haberleşmesi ve karmaşık elementlerin davranışı sanallaştırılabilir ve anlaşılabilir. Aynı zamanda bu program, açık

kaynak kodlu ve UNIX, Windows, MacOs gibi farklı işletim sistemlerinde çalıştığı için yaygın olarak kullanılmaktadır.

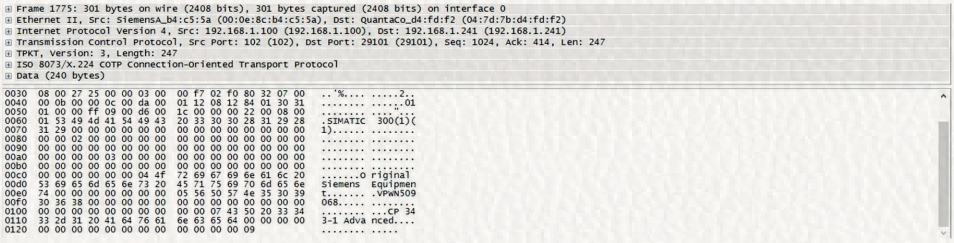
Modbus, Profibus, DNP3 gibi endüstriyel kontrol sistemlerinin haberleşmesi için kullanılan birçok protokol Wireshark tarafından desteklenmekte ve bu protokollerin davranışları sanallaştırılabilmektedir. Şekil 13.7 ve Şekil 13.8'de Gazi Üniversitesi SCADA Laboratuvar ortamında tasarlanan Modbus ve Profinet haberleşmelerinden elde edilen Wireshark görüntüleri mevcuttur.



Şekil 13.7. Modbus Wireshark görüntüsü

Şekil 13.7'de verilen Wireshark görüntüsünde Modbus protokolüne yönelik yakalanan paketler gösterilmiştir. Modbus protokolünün fonksiyon kodu ve bu fonksiyon koduyla endüstriyel kontrol sistemine gönderilen veri gösterilmiştir.

Şekil 13.8'de çalışmada kullanılan Siemens Simatic S7-300 cihazının Profinet Protokolü'ne yönelik yakalanan paketleri gösterilmiştir. S7-300 CPU cihazı kullanılan çalışmada Şekil 13.8'den de görüldüğü üzere CP 343-1 Advanced haberleşme modülü kullanılmıştır.



Şekil 13.8. Profinet Wireshark görüntüsü

13.3.3. Nmap Ağ Tarama Aracı

Nmap, TCP/IP tabanlı çalışan bilgi sistemlerinin açık port ve servisleri gibi potansiyel zafiyetlerini taramak için kullanılan açık kaynak kodlu çok amaçlı bir tarama aracıdır [24]. Aynı zamanda ağ topolojisinin çıkarılması için de kullanılmaktadır. Zafiyet değerlendirmesinin ve bilgi toplama fazının önemli bir kısmı port taramasıyla gerçekleştirilir. Her bir makinanın açık portlarının listesi SCADA sistemine zafiyetlerini istismar edip sızmak için bir adım teşkil eder. Şekil 13.9'da Siemens S7-1200 PLC cihazının kullanıldığı deney düzeneği ortamında nmap taraması sonucu elde edilen açık portların ve servislerin listesi görülmektedir. Yapılan tarama sonucunda varsayılan olarak 102. port üzerinde Profinet Protokolü'nün ve iso-tsap servisinin çalıştığı görülmektedir.

```
root@kali:~/Desktop# nmap -sS -T5 192.168.1.100 -p 102 -n

Starting Nmap 6.47 ( http://nmap.org ) at 2015-11-18 18:07 EET
Nmap scan report for 192.168.1.100
Host is up (0.00041s latency).
PORT    STATE SERVICE
102/tcp open  iso-tsap

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

Şekil 13.9. Nmap taraması

13.3.4. Plcscan Aracı

Plcscan, ScadaStrangeLove grubu tarafından yayımlanan bir yardımcı programdır. PLC cihazlarının ve ağ üzerindeki diğer Modbus cihazlarının tespitinde kullanılır [25].

Plcscan, TCP/102 ve TCP/502 portlarının durumlarını kontrol etmek için yazılmış bir Python scriptidir. Eğer bu iki portu açık bulursa, bu portlarla ilgili diğer fonksiyon veya scriptleri çağırır. Örneğin TCP/502 portunun açık olduğunu tespit ederse, cihazın tanınması için MEI tipini çekerek Modbus

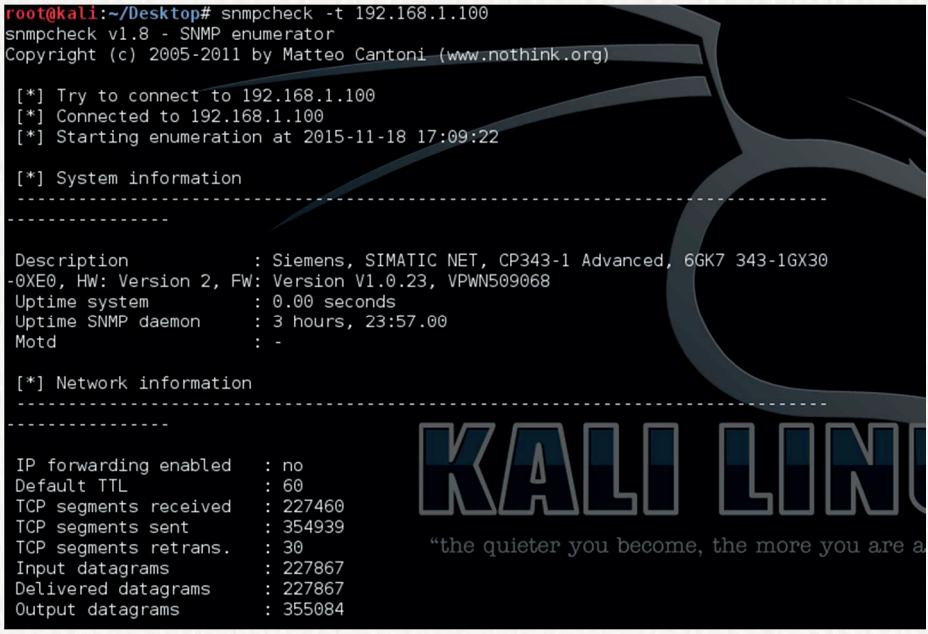
fonksiyonlarını çağırır. Daha sonra cihazın kimliği dönecek ve dönen bu bilgi ekranda görüntülenecektir.

Plcscan, PLC cihazından hızlı sonuç alan temel bir araçtır. Bilgiler doğrudan cihazdan çekilir ve benzeri cihazlarda ilk test olmadan kullanılırsa bazı sorunlara neden olabilir. Bazı konularda sınırlama gerektiren kod içinde bazı hata kontrollerini yapmaktadır. Plcscan tarafından toplanan bu bilgiler Profinet ve Modbus protokollerinin olduğu iki çıkış şeklinde olabilir. Bu cihazlardan toplanan çıktılar donanım yazılımı versiyonlarını içermektedir. Şekil 13.10'da Siemens S7-300 PLC cihazının bulunduğu deney düzeneği ortamında plcscan tarama sonuçları gösterilmiştir. Tarama sonuçlarına göre kullanılan cihazın modül tipi, seri numarası, projede kullanılan modülün ve plc cihazının adı versiyonu ve donanım bilgileri elde edilmiştir.

Şekil 13.10. Plcscan tarama sonuçları

13.3.5. Snmpcheck

Snmpcheck komutunun amacı, Windows, Unix, ağ cihazları, yazıcılar ve PLC cihazları gibi Snmp protokolünü destekleyen herhangi bir cihazın bilgi toplama işleminin otomatize edilmesidir. Snmpcheck, snmp cihazlarını listelemeye ve okunur bir şekilde çıktı alınmasına imkân verir. Sistem izleme veya sızma testlerinde oldukça kullanılmaktadır. Snmpcheck komutuyla çalışmada kullanılan S7-300 cihazından elde edilen bilgiler Şekil 13.11'de gösterilmiştir. Elde edilen sonuçlara göre CP 343-1 İleri (Advanced) haberleşme modülünün detaylı versiyon bilgisi ve cihazın ne kadar süredir çalışmakta olduğu gözükmektedir.



Şekil 13.11. Snmpcheck komutu sonuçları

13.3.6. Metasploit Framework

Metasploit Framework bilgi güvenliği toplulukları arasında en yaygın ve en bilinen sızma testi araçlarından birisidir. H. D. Moore tarafından 2003 yılında ilk versiyonu yayımlanmıştır. 2007 yılında Moore bu projede perl dilinden vazgeçip ruby kodunda en baştan tekrar yazmıştır. 2009 yılında Rapid7 güvenlik firması bütün Metasploit Projesi'ni satın almıştır.

Metasploit Framework'ü istismar kodu geliştirme toplulukları için yaygın bir şekilde kullanılmaktadır. Güvenlik uzmanları ve geliştiricileri açık kaynak kodlu platformu geniş altyapılı bilgi sistemlerini test etmek ve belirli hedef sistemler için yeni istismar kod yazmak için kullanmaktadırlar. Mevcut durumda içerisinde farklı sistemler ve yazılımlar için 1800'den fazla istismar kodu bulunmaktadır.

İstismar kodunu başarılı bir şekilde çalıştırmak için 4 temel adım mevcuttur. Bu adımların açıklamaları aşağıda verilmiştir:

İstismar kodu yapılandırması: Hedef sisteme veya yazılıma yönelik saldırı türü seçilir.

Payload yapılandırması: İstismar kodunun çalışması için hedef makine üzerinde hangi kodun çalıştırılacağı belirlenir.

Enkodlama yapılandırması: IPS/IDS sistemlerinden korunmak için yapılacak işlem belirlenir.

İstismar kodunun çalıştırılması: Saldırı işlemi başlatılır ve hedef sistemle haberleşme kanalı açılır.

Scadahacker'ın düzenlemiş olduğu SCADA sistemlerinin zafiyetlerine yönelik yazılmış metasploit modüllerinin bir kısmı Tablo 13.3'te gösterildiği gibidir.

Tablo 13.3. SCADA sistemleri için hazırlanmış metasploit modüllerinden bazıları [26]

Araç/İstismar Kod Adı	Geliştirici	Sistem	Metasploit Referans
teechart_pro.rb	BACnet	Operator Workstation	exploit/windows/browser/teechart_pro .rb
simatic_s7_1200_command.rb	Dillon Beresford	Siemens Simatic S7 module	Açık kaynak olarak indirilmektedir.
simatic_s7_300_command.rb	Dillon Beresford	Siemens Simatic S7 module	Açık kaynak olarak indirilmektedir.
modbusclient.rb	EsMnemon and Arnaud Soullie	Modbus Client Utility	auxiliary/scanner/scada/modbusclient.r b
modbusdetect.rb	EsMnemon	Modbus Client Utility	auxiliary/scanner/scada/modbusdetect. rb

13.3.6.1. Modbusdetect Modülü

Çalışmanın bu bölümünde, yukarıda bahsedilen Metasploit Framework modüllerinden modbusdetect ve modbusclient modülleri kullanılarak hedef sistem üzerinde Modbus Protokolü'nün tespiti ve üzerindeki yazmaçlarda yazan değerleri okuyup değiştirme işlemleri yapılacaktır.

Şekil 13.12'de modbusdetect modülü kullanılarak hedef sistem üzerinde bilgi toplama amaçlanmıştır. Modbusdetect Metasploit modülü, hedef sistemde

koşan Modbus/TCP protokolünü taramak ve tanımlamak için belirli bir IP adresi aralığındaki Modbus servislerini tespit eder. Bu modül Modbus istek paketlerini hedef sistemin 502. portuna göndererek tespit eder ve aynı İşlem ID ve Protokol ID içeren yanıtları bekler. Modül Modbus/TCP başlığı ve PLC cihazının Birim ID'sini döndürür [27].

```
msf auxiliary(modbusdetect) > show options

Module options (auxiliary/scanner/scada/modbusdetect):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   RHOSTS                     yes       The target address range or CIDR identifier
   RPORT     502              yes       The target port
   THREADS   1                yes       The number of concurrent threads
   TIMEOUT   10               yes       Timeout for the network probe
   UNIT_ID   1                yes       ModBus Unit Identifier, 1..255, most often 1

msf auxiliary(modbusdetect) > set RHOSTS 192.168.206.132
RHOSTS => 192.168.206.132
msf auxiliary(modbusdetect) > run

[+] 192.168.206.132:502 - MODBUS - received correct MODBUS/TCP header (unit-ID: 1)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Şekil 13.12. Modbusdetect modülü

13.3.6.2. Modbusclient Modülü

Modbusclient, PLC üzerindeki verileri Modbus/TCP Protokolü'nü kullanarak okumaya veya yazmaya yarayan Metasploit modülüdür. Orijinal modbusclient modülü EsMnemon tarafından protokolün Fonksiyon Kodu'nu 0x06 kullanan salt-yazılır modülüydü ("Write Single Register"). Arnaud Soullie; 0x01 (Read Coil), 0x03 (Read Holding Register) ve 0x05 (Write Single Coil) fonksiyon kodlarını dâhil etmek için kod üzerinde değişiklikler yapmıştır [28].

Fonksiyon Kodu 0x01 (Read Coil) kullanılarak başarıyla çalıştırılan modbusclient modülü kullanıcıya uzak PLC cihazındaki 1-2000 arasında komşu sarmalların durumunu okumasına olanak sağlar. Şekil 13.13'te gösterilen DATA_ADDRESS bölümü, döndürülen bobin durumu (0x0000 – 0xFFFF) için 2 baytlık başlangıç adresini belirtir. Modbus sunucusundan dönen cevap veri alanında her bobin için bir biti temsil eden bobin durumudur [29].

Fonksiyon Kodu 0x03 (Read Holding Register) kullanılarak başarıyla çalıştırılan modbusclient modülü kullanıcıya uzak PLC cihazındaki 1-2000 arasın-

da komşu yazmaç girişleri okumasına olanak sağlar. Şekil 13.14'te gösterilen DATA_ADDRESS bölümü döndürülen yazmaç durumu (0x0000 – 0xFFFF) için 2 baytlık başlangıç adresini belirtir. Modbus sunucusundan dönen cevap, cevap mesajında her yazmaç için iki baytlık yazmaç değeridir [29].

Fonksiyon Kodu 0x05 (Write Single Coil) kullanılarak başarıyla çalıştırılan modbusclient modülü kullanıcıya uzak PLC cihazının bobinine tek çıktı (ON veya OFF) yazmaya olanak sağlar. Şekil 13.14'te gösterilen DATA alanı kullanılarak girdi veri değeri, çıktının ON olması için 0xFF00 değerini, OFF olması için 0x0000 değerini kabul eder. Diğer tüm girdi değerleri geçersizdir ve çıktıyı etkilemeyecektir [29].

Fonksiyon Kodu 0x06 (Write Single Register) kullanılarak başarıyla çalıştırılan modbusclient modülü kullanıcıya uzak PLC cihazındaki tekli meşguliyet yazmacına (single holding register) yazmasına olanak sağlar. Şekil 13.13'te gösterilen DATA_ADDRESS alanı yazılacak yazmaç adresini tanımlar (0x0000 – 0xFFFF). Bu isteğin başarılı bir şekilde çalıştırılması tanımlanan DATA alanının değerini yankılar [29].

Çalışmada *Modbusclient* modülü kullanılarak hedef sistemde yazmaç üzerindeki değerler sırasıyla Şekil 13.13 ve Şekil 13.14'te görüldüğü üzere okunabilmiş ve değiştirilebilmiştir.

```
msf auxiliary(modbusclient) > show options

Module options (auxiliary/scanner/scada/modbusclient):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   DATA                           no        Data to write (WRITE_COIL and WRITE_REGISTER mode
   DATA_ADDRESS  2                yes       Modbus data address
   RHOST         192.168.206.132  yes       The target address
   RPORT         502              yes       The target port
   UNIT_NUMBER   1                no        Modbus unit number


Auxiliary action:

   Name           Description
   ----           -----------
   READ_REGISTER  Read one word from a register


msf auxiliary(modbusclient) > run

[*] Sending READ REGISTER...
[+] Register value at address 2 : 402
[*] Auxiliary module execution completed
```

Şekil 13.13. Modbusclient READ_REGISTER aksiyonu

```
msf auxiliary(modbusclient) > show options

Module options (auxiliary/scanner/scada/modbusclient):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   DATA          2016             no        Data to write (WRITE_COIL and WRITE_REGISTER mode
   DATA_ADDRESS  2                yes       Modbus data address
   RHOST         192.168.206.132  yes       The target address
   RPORT         502              yes       The target port
   UNIT_NUMBER   1                no        Modbus unit number


Auxiliary action:

   Name            Description
   ----            -----------
   WRITE_REGISTER  Write one word to a register


msf auxiliary(modbusclient) > run

[*] Sending WRITE REGISTER...
[+] Value 2016 successfully written at registry address 2
[*] Auxiliary module execution completed
```

Şekil 13.14. Modbusclient WRITE_REGISTER aksiyonu

13.4. LİTERATÜRDEKİ KRİTİK ALTYAPILARA YÖNELİK SİBER SALDIRILAR

Bilgi ve iletişim teknolojisinin gelişmesiyle birlikte haberleşme, ulaşım, enerji ve otomasyon gibi kritik altyapı sistemleri bu teknolojiyle entegre çalışır hâle gelmiştir. Dolayısıyla bilgi teknolojilerinde oluşabilecek güvenlik açıkları direk olarak bilgi teknolojileri altyapısını kullanan kritik altyapı sistemlerini de etkileyebilmekte ve risk teşkil edebilmektedir. Bu yüzden bilgi sistemlerine zarar vermek için kullanılan kötücül yazılımlar kritik altyapı sistemlerine zarar vermek için de kullanılabilmektedir. Bu sistemlere yönelik yapılan siber saldırıların motivasyonu genellikle siyasi olmakta ve amacı hedef alınan ülkenin kritik altyapılarına ve projelerine zarar vermektir.

Çalışmanın bu bölümünde ülkelerin toplum ve kamu düzenini ve ulusal güvenliğini ilgilendiren kritik bilgi sistemlerine yönelik gerçekleştirilmiş siber saldırılar incelenmiştir.

13.4.1. Sibirya Boru Hattı Patlaması

1982 yılında yeni inşa edilmiş trans-Sibirya boru hattının büyük bir kısmını buharlaştırarak Sibirya'nın ortasında bir patlama meydana gelmiştir. Bu patlama 2. Dünya Savaşı'nda Japonya'ya atılan nükleer bombanın 1/7 oranında bir etki yaratmış ve Sovyetler Birliğine petrol gelirinden 8 milyar dolar gelir getiren boru hatları ciddi oranda zarar görmüştür. Yalnız son zamanlarda CIA tarafından gerçekleştirildiği kamuoyuna duyurulmuştur [30].

CIA yetkilisinin yaptığı açıklama şu şekildedir: "Böyle muazzam bir tesisteki vanalar, kompresörler ve depolama alanlarının çalışmasını otomatik hâle getirmek için Sovyetler karmaşık kontrol sistemlerine ihtiyaç duymuşlardır. Rus boru hattı yetkilileri gerekli yazılım için ABD'ye yakınlaştı fakat geri çevrildiler. Ruslar yılmadan başka yerlere baktı; KGB gerekli kodları çalmak için Kanadalı yazılım tedarikçisine sızma girişiminde bulundu. Amerika istihbaratı ve Rus istihbaratına çift taraflı olarak çalışan Vladimir Vetrov (Kod Adı: Farewell) bu duruma sinirli bazı Kanadalılarla iş birliği içindedir. Boru hattının yazılımı; pompaların, tribünlerin ve vanaların çalışmasını saptırmak içindir. Bir süre sonra pompa hızlarını ve vana ayarlarını sıfırlar ve boru hattının kaynaklarına ve bağlantılarına giden kabul edilebilir basıncı üretir. Sonucunda uzaydan görülebilecek düzeyde devasa bir patlama oldu. Beyaz Saray, kızılötesi uydularından Sovyetler'in ortasında bazı olağan dışı uyarılar aldıklarını belirtti [31]."

13.4.2. The Salt River Proje (SRP) Ele Geçirme Olayı

1994 yılında Lane Jarrett Davis, Salt River Projesi (SRP) bilgisayar ağına çevirmeli modem üzerinden yetkisiz erişim sağlamış ve fatura bilgilerine erişmiştir. Sisteme daha sonra girebilmesi için arka kapı bırakmıştır. Aynı zamanda, SRP SCADA sistemi Phoenix'teki müşterilere su dağıtımı için kullanılan yaklaşık 210 km'lik kanalı kontrol etmektedir. Mr. Davis kanalları kontrol eden kritik sistem üzerinde en az 5 saatlik bir oturum açmıştır. Su ve güç izleme ve dağıtımı, finans, müşteri ve kişisel bilgileri içeren korumasız verileri ele geçirmiştir. Login ve parola dosyaları, bilgisayar sistem kayıt dosyaları ve "root" yetkilerini ele geçirmiştir. Dahası, SRP ve Ulusal Meteoroloji Servisi'nin Ulusal Şiddetli Fırtına Laboratuvarı arasındaki Doppler-radar araştırma projesine de erişmiştir. SRP, bu saldırı nedeniyle düşük verimliliği hariç tahmini 40,000 $ kayba uğramıştır [32].

Bu sızma olayı Roosevelt Barajı'na yapılan saldırıyla bağlantılıdır ve sürekli olarak gündeme gelen bir efsane hâline gelmiştir. Daha önce ABD Temsilciler Meclisi'nin yaptığı açıklamada "bir çocuk korsan Arizona'da Roosevelt Barajı'nın faaliyetlerini kontrol eden firmaların ağına yetkisiz erişim sağladı" denmiştir. Aynı zamanda bu saldırı yapıldığında Mr. Davis 27 yaşındaydı ve SRP ve Roosevelt Barajı arasında bir bağlantı olmadığı belirtilmektedir.

13.4.3. Houston Limanı Sistem Arızası

2001 yılında genç bir bilgisayar korsanı (Aaron Caffrey), bir bayan sohbet odasını hedef almak için Texas'taki Houston Limanı bilgisayar sunucularına sızmıştır. Saldırıda, dünyanın en büyük 8. limanında düzenleme yapmak için kullanılan bilgisayar sistemlerine hizmet dışı bırakma saldırısı yapılmıştır. Gemi kaptanları için kritik bilgiler içeren limanın web servisi hizmet dışı kalmıştır. Bu yüzden gemilerin navigasyon bilgileriyle limandan giriş ve çıkışlarından sorumlu olan demirleme ve destek firmaları hizmet veremez duruma gelmiştir [33].

13.4.4. Slammer Solucanı

2003 Mayıs'ta kurumsal bir firmada çalışan bir personel, Microsoft SQL versiyonun güncel olmadığının farkına varmadan dizüstü bilgisayarına bir yazılım yüklemiştir. Bir süre sonra, kullanıcı bir internet servis sağlayıcı üzerinden e-posta sunucusuna erişmek için bilgisayarını internete bağlamıştır (şirket politikalarını çiğneyerek). Böylece SQL-slammer solucanı internete bağlı olan makinaya bulaşmıştır. Çalışan daha sonra bilgisayarını ofise getirmiş ve ağa bağlanmıştır. Böylece SQL-slammer solucanı kurumsal ağa bulaşmıştır [34].

Güvenlik duvarı olmayan ve veri toplama sunucusu olan kontrol sistemi ve geliştirme kontrol sistemi enfekte olmuştur. Bu durumda daha fazla bulaşma olmadan sunucu kontrol ağından çıkartılmak zorunda kalınmıştır. Üretimde ciddi bir etki olmamıştır fakat bazı geçmiş veriler sunucunun durması sürecinde kaybedilmiş ve tekrar manuel olarak oluşturulmak durumunda kalınmıştır.

13.4.5. Kaliforniya Kanal Sisteminin Hacklenmesi

Kaliforniya Kanal Sistemi'nin bir çalışanı Sacramento Nehri'den suyu yönlendirmek için kullanılan bilgisayara yetkisiz bir yazılımı yüklemekten ve

zarar vermekten yargılanmıştır. 61 yaşındaki Tehama Colusa Kanal Otoritesi (TCAA) elektrik danışmanı olan Michael Keehn, "yetkisiz bir şekilde kasten korunan bir bilgisayara zarar vermekten" 10 yıl hapis cezasına çarptırılmıştır.

İddialara göre; Keehn, TCAA'daki SCADA sistemine yetkisiz bir yazılımı yüklemiştir. Bu sisteme erişimi 15 Ağustos 2007 yılındadır. Elektrik danışmanı olarak TCAA'daki bilgisayar sistemlerinden sorumludur. 16 personelle birlikte TCAA Kaliforniya'daki tarımsal alanlar için Tehama Colusa ve Corning Kanalı olmak üzere 2 kanalı kontrol etmektedir. Her iki sistem de devletin hüküm ve tasarrufundadır. ABD Adalet Bakanlığı temsilcilerinden Robin Taylor; TCAA SCADA sistemlerine bir saldırı olmasında sistem çevrim dışı kalsa bile kanallar çalışmaya devam eder demiştir. Bilgisayarlar çalışmadığı zaman manuel olarak çalıştırılırlar. Bu sızmanın TCAA'ya 50,000 $'dan fazla zararı olmuştur [35].

13.4.6. ABD'de Elektrik Şebekesi Casusluk İhlali

Wall Street Gazetesi 2009 Nisan'da Rus ve Çinli casusların Amerika elektrik şebekesine sızdıklarını yazmıştır [36]. Milletvekilleri kaçınılmaz tehditlerle mücadele etmek için hükümete yetki verecek tedbirlerin dâhil olduğu elektrik sektöründe siber güvenliği arttıracak teklifler getirmişlerdir.

Elektrik endüstrisinde siber güvenlik danışmanı Bob West, NERC'in endüstrinin proaktif olması konusunda teşvik edici olduğuna dikkat çekmiştir.

13.4.7. Nitro Saldırıları

Nitro saldırıları öncelikle kimyasal ve gelişmiş materyaller üzerinde çalışan, araştırma, geliştirme ve üretim firmalarını hedef almıştır. Saldırganların amacı endüstriyel espiyonaj yapmak, tasarım dokümanları, formülleri ve üretim süreçleri gibi fikri mülkiyetleri toplamaya yöneliktir.

Saldırının metodolojisinde, saldırganlar hedef aldıkları firmaların çalışanlarına içerisinde kötücül eklenti bulunan bir e-posta göndermişlerdir. E-posta içerikleri iş ortağıyla davetiye paylaşmak ve güvenlik güncelleme zamanlarının geldiğiyle ilgilidir. Firma çalışanı e-posta içeriklerini açtıklarında çalıştırılabilir dosya bir arka kapı oluşturur ve bu Truva atı Çin merkezli bir C&C sunucuyla 80. port üzerinden şifreli bir şekilde iletişim kurar. Saldırgan böylece etki alanındaki Windows makinaların parola özetlerini ele geçirir [37].

13.4.8. Stuxnet Solucanı

Stuxnet solucanı; siber güvenlik camiası tarafından "ezber bozan" (game-changer) kötücül bir yazılım olarak tanımlanmaktadır [38]. Çünkü, bu kötücül yazılımın karmaşıklığı, amacı ve çıkarımları diğer kötücül yazılımlardan farklıdır. Stuxnet solucanının gelişimi ve yayılımı siber teknolojinin, dünya politikasına yön verebilecek bir tehdit olabileceğini göstermiştir.

Stuxnet solucanı, diğer bilgisayar solucanları gibi güvenlik açığı olan bir bilgisayardan bir diğerine ayrım gözetmeksizin yayılmaktadır. Diğer binlerce bilgisayar solucanından ayıran en büyük özelliği Natanz'da İran'ın nükleer zenginleştirme tesisinin özellikleriyle eşleşen sadece Endüstriyel Kontrol Sistemi'ne (ICS) girdiğinde kendi yükünü ortaya çıkarmak için tasarlanmış olması ve içerisinde 4 adet Windows işletim sistemlerini istismar eden 0 gün zafiyeti bulunmasıdır. Bu gerçekleştiğinde, Natanz'daki santrifüjlerin kontrolü için kullanılan Programlanabilir Mantıksal Denetleyicilerin (PLC) kodlarını kurcalar. Nihayetinde binlerce santrifüj zarar görmüş ve İran Nükleer faaliyetleri sekteye uğramıştır. Daha önce hiçbir solucan ICS üzerinden fiziksel olarak sistemlere zarar verememiştir.

Stuxnet solucanı, içerdiği fonksiyon ve yapısından dolayı kritik altyapılara yönelik gerçekleştirilen diğer siber saldırılardan daha farklı bir boyutta değerlendirilmelidir. Bu yüzden, bu bölümde Stuxnet'e ait ayrı bir değerlendirme bölümü yapılmıştır.

Knopová çalışmasında [39], 3. Dünya Savaşı'nın siber uzayda gerçekleşebileceğinden bahsetmektedir. Konvansiyonel silahların ve savaşların maddi ve manevi maliyeti çok ciddi rakamlara ve insan hayatına mal olabileceğinden siber savaş gerçeği bu tezi doğrular niteliktedir. Özellikle bu çalışmada anlatılan Stuxnet solucanı ile saldırıyı gerçekleştiren taraf hedef sisteme sızma ve zarar verme işlemini başarıyla gerçekleştirmiş ve bu saldırıyı kaynağını gizleyerek gerçekleştirmiştir. Bu sayede normalde savaş sebebi sayılabilecek bir saldırı yapmaktan ve can kaybına sebebiyet vermeden sadece hedef sistemlere zarar vermiştir. İran yapılan bu saldırıdan sonra saldırının kaynağı olarak iddia edilen ABD ve İsrail'e karşı hukuki bir süreç başlatamamıştır. Çünkü bahsedildiği gibi yapılan saldırının kaynağı ABD ve İsrail'i işaret etmemektedir.

Yukarıda anlatıldığı gibi Stuxnet solucanı içerisinde bulundurduğu 4 adet 0-gün güvenlik açığı ve o güne kadar keşfedilmiş en karmaşık kötücül yazı-

lım olmasından dolayı kötücül yazılım analizcilerine yeni bir alan açmış ve tüm dünyada büyük ses getirmiştir. Aynı zamanda endüstriyel kontrol sistemlerinin denetimini sağlayan PLC cihazlarına yönelik gerçekleştirilmesi kritik altyapıların siber ortamdan korunması ve güvenliğine yönelik yeni çözüm önerilerinin doğmasına ve farkındalığın artmasına imkân sağlamıştır.

13.4.9. Duqu Truva Atı

2011 yılında Word dokümanlarına yönelik Duqu saldırıları, içerisinde 0-gün açığı bulunan (CVE-2011-3402) güvenlik açığı tespit edilmiştir. Bu istismar saldırganlara bir Word dokümanından kernel moda atlamasına olanak sağlar. Word dosyası açıldığında istismar modülü tetiklenmiş olur ve bu istismar HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\InternetSettings\Zones\4\"CF1D" kayıt değerine bakarak ilk olarak bilgisayarın ele geçirilip geçirilmediğini kontrol eden kernel mod shellcode barındırır. Bilgisayar ele geçirildiyse, shellcode mevcuttur. Ele geçirilmediyse; shellcode, Word dokümanından iki çalıştırılabilir dosyanın şifresini çözer: bir driver dosyası ve installer DLL. Daha sonra yükleyici yapılandırma dosyası tarafından tanımlanan services.exe içine kodu enjekte eden çıkarılmış yükleyici dosyasına çalışmayı geçirir. Kod daha sonra installer DLL'i çalıştırır. Sonunda, shellcode kendini hafızadan silerek sıfırlarla yer değiştirir [40].

13.4.10. Shamoon Zararlı Yazılımı

15 Ağustos 2012 tarihinde Suudi Arabistan'ın millî petrol üretimi, satışı, ham petrol rafinerisi, doğal gaz ve petrol ürünleri firması olan Suudi Arabistan Petrol Firması'nın (Saudi Aramco) yaklaşık 30,000 Windows işletim sistemi tabanlı bilgisayar ağına bir bilgisayar virüsü bulaşmıştır. Saudi Aramco, dünya petrol pazarında çok büyük bir paya sahiptir. Global arzın %10'nu, global üretimin %13'nü elinde tutan ve yıllık 200 milyar $ geliri olan dünyanın en büyük petrol üreticisidir.

Shamoon kötücül yazılımı Aramco'daki çalışanların kişisel bilgisayarlarına bulaşmış ve bilgisayarların hard disklerindeki verileri fark gözetmeksizin silmiştir. Herhangi bir petrol sızıntısı, patlaması veya daha büyük bir arızanın olmamasına rağmen bu saldırı firmanın üretim bilgilerinin silinmesi gibi üretim ve iş faaliyetlerini ciddi oranda etkilemiştir. Shamoon aynı zamanda

RasGas, Qatar Petrol ve ExxonMobil gibi diğer gaz ve petrol firmalarına yayılmıştır.

Shamoon saldırısı Orta Doğu'da herhangi bir fiziksel hasara sebebiyet vermese de dünya çapında kritik servis sağlayıcıları için risk değerlendirmesine ikincil etkileri olmuştur. Bu olay ABD ve İran arasında ciddi güvenlik kaygılarını arttırmıştır. Dönemin ABD Savunma Bakanı Leon Panetta, Shamoon için "çok karmaşık" ve "bu tip araçların kullanımı çok endişe verici" şeklinde açıklama yapmıştır [41].

13.4.11. Flame Zararlı Yazılımı

Flame virüsü oldukça gelişmiş, Microsoft Windows işletim sistemi tabanlı çalışan bilgisayarlara bulaşan ve casusluk amacıyla yazılan bir yazılımdır. Aynı zamanda, yerel bilgisayar ağları içinde yayılmak için gereken mekanizmalardan biri oldukça dikkat çekicidir. Kendisini Windows güvenlik güncellemesi olarak saklayarak, Windows güncelleme üzerinden yerel ağ üzerinden yayılır.

Budapeşte Üniversitesi CrySyS Lab.'ın yapmış olduğu teknik rapora göre; Flame, klavye girdileri, ekran görüntüleri ve mümkünse mikrofon ve kamera görüntüleri gibi bilgileri toplamaktadır. İlk bulaşmasından sonra indirilebilen birçok modülü mevcuttur. Tamamen yapılandırılmış boyutu 20 mb'tan fazladır. Bu boyut bir kötücül yazılım için oldukça fazladır. Flame, Windows güncellemeyi kullanarak ağlar arasında yayılır ve aynı zamanda çıkarılabilir sürücü ile hava boşluğunu aşabilir. Flame bir ağ içerisinde bir bilgisayara bulaştığında, kendisini *update.windows.com* için vekil sunucu olarak kaydetmek için WPAD'i (Web Proxy Auto-Discovery Protocol) kullanır ve kendisini ağdaki diğer bilgisayarlara yüklemek için sahte güvenlik güncellemesi hizmeti verir [42]. Flame hızlı bir şekilde yayılmaz, büyük çoğunluğu Orta Doğu'da olmak üzere çok az sayıda bilgisayar bu kötücül yazılımdan etkilenmiştir. İlk varyasyonu İran (CERT) tarafından 2012 Mayıs'ında bulunmuştur. Kaspersky'a göre; en az 2010 yılına kadar aktifti fakat CrySys Lab, 2007 yılında bilgisayar güvenliği firması olan Webroot tarafından bulunan ve Flame'de kullanılan dinamik bağlantı kütüphanesinin adı olan WAVESUP3.DRV dosya ismini raporlamıştır. Bu durum Flame'in veya daha önceki varyasyonlarının o dönemde zaten aktif olduğunu göstermektedir. Bu yazılımın bulaştığı bilgisayarların büyük çoğunluğu İran coğrafyasındaydı. Hedefleri arasında devlet kurumları, özel firmalar, eğitim

enstitüleri ve belirli bireyler bulunmaktadır. *The Washington Post* gazetesinde [43] Flame veya benzeri Stuxnet gibi kötücül yazılımların ABD ve İsrail tarafından geliştirildiği iddia edilmektedir.

13.4.12. Doğalgaz Boru Hattı Firmalarına Siber Saldırılar

2012 yılında 6 ay boyunca, kimliği tam olarak belirlenemeyen (Çin kaynaklı olduğu iddia edilmekte) bir hacker grubu tarafından ABD gaz boru hatlarının kontrol sistemlerine devamlı ve eşgüdümlü bir şekilde siber saldırı düzenlenmiştir. Saldırganlar "spear-phishing" tekniğini kullanarak boru hattı kontrol sistemlerine erişim sağlayıp parolaları çalmayı hedeflemişlerdir. Saldırganlar gönderdikleri e-postaları hedef aldıkları kişilerin arkadaşı veya tanıdığı birinden geliyormuş gibi yapmışlar ve e-postadaki eklenti veya link açıldığında kötücül yazılım hedef bilgisayara bulaşmıştır.

ABD İç Güvenlik Bakanlığına göre gönderilen spear-phishing'lerin ilki Mart 2012'de tespit edilmiş ve gaz firmasındaki küçük bir çalışan grubu hedef almıştır [44].

13.4.13. Ukrayna Elektrik Kesintisi

23 Aralık 2015 tarihinde Ukrayna'da Ivano-Frankivsk bölgesindeki yerleşkelerin yaklaşık yarısı (1,4 milyon insan) birkaç saatlik elektrik kesintisi yaşamışlardır. ESET firmasındaki siber güvenlik araştırmacılarına göre bu kesintinin sebebi bir siber saldırıdır [45].

ESET çalışanlarına göre; saldırganlar, yeniden önyükleme yapamayacakları şekilde tasarlanan hedef bilgisayarlardaki KillDisk bileşenine "*BlackEnergy*" arka kapısını kullanarak saldırılarını gerçekleştirmişlerdir.

BlackEnergy arka kapısı, truva atı modüler yapısından oluşmakta ve belirli görevleri yürütmek için çeşitli indirilebilir bileşenleri kullanmaktadır. 2014 yılında, Ukrayna'da yüksek profilli devlet kurumlarına karşı bir dizi siber casusluk faaliyetlerinde kullanılmıştır. Elektrik dağıtım şirketlerine karşı son saldırılarda, KillDisk Truva atı indirilmiş ve daha önce BlackEnergy Truva atı bulaşmış sistemler üzerinde çalıştırılmıştır.

BlackEnergy ve KillDisk arasındaki ilk bağlantı Kasım 2015'te Ukrayna CERT-UA tarafından raporlanmıştır. Bu sırada birçok medya kuruluşu Ukray-

na yerel seçimleri sırasında saldırıya uğramıştır. Raporda bu saldırılar sonucunda çok sayıda video materyallerinin ve çeşitli dokümanların tahrip olduğu iddia edilmiştir.

Ukrayna güç dağıtım firmalarına yönelik gerçekleştirilen saldırılarda kullanılan KillDisk varyasyonu bazı ek fonksiyonlara sahiptir. Sistemin önyükleme yapamaması için sistem dosyalarını silmesinin yanı sıra bu özel varyant endüstriyel kontrol sistemlere sabotaj düzenlemek için tasarlanmış kodlara sahiptir.

ESET zararlı yazılım analisti Anton Cherepanov; "KillDisk'in normal fonksiyonlarının haricinde aynı zamanda Endüstriyel Kontrol Sistemlerinde sıkça kullanılan platformlara ait işlemleri sonlandırmaya çalıştığını" söylemektedir [45].

Bu işlemler hedef sistemde bulunursa, Truva atı bu işlemleri sadece durdurmaz aynı zamanda sistemin yeniden çalışmasını zorlaştırmak için rasgele verilerle hard disk üzerinde ilgili çalıştırılabilir dosyayı yazar.

Cherepanov aynı zamanda "Ukrayna'da birçok elektrik dağıtım firmalarında tespit edilen KillDisk kötücül yazılımı üzerinde yaptığımız çalışmalar, Kasım 2015'te Ukrayna medyasına düzenlenen saldırılarda kullanılan araçlarla aynı olduğunu göstermektedir" demiştir [45].

13.4.13.1. BlackEnergy'nin 2015'teki Gelişimi

BlackEnergy aktif olduğunda, BlackEnergy varyantları enfekte bilgisayarın gerçekten istenilen hedef olup olmadığını değerlendirmek amacıyla belirli kriterleri kontrol etmeye olanak sağlar. Bu durumda, normal bir BlackEnergy varyantının damlalıkları (dropper) sisteme itilir.

C&C sunucularından farklı olarak BlackEnergy yapılandırması "build_id" değerini barındırır. Bu değer BlackEnergy kötücül yazılımı operatörü tarafından bulaşma girişimini veya ayrı bulaşmaları tanımlamak için kullanılan benzersiz bir metin dizesidir. Harflerin ve sayıların kombinasyonları hedef sistem hakkında açığa çıkan bilgileri kullanabilir.

ESET tarafından 2015 yılında Ukrayna'ya düzenlenen saldırıda tanımlanan "build_id" değerleri aşağıdaki gibidir:

- 2015en
- khm10

- khelm
- 2015telsmi
- 2015ts
- 2015stb
- kiev_o
- brd2015
- 11131526kbp
- 02260517ee
- 03150618aaa
- 11131526trk

Bu değerlerden bazıları belirli anlamlara gelmektedir. Mesela "2015telsmi" değeri Rusçada Sredstva Massovoj Informacii (Kitle İletişim Araçları, SMI) kısaltması veya "2015en" enerji anlamına gelebilir.

13.4.13.2. Killdisk Bileşeni

2014 yılında, bazı BlackEnergy varyantları "dstr" isimli enfekte olmuş sistemi çökertmek için tasarlanmış eklenti barındırıyordu. 2015'te ESET, BlackEnergy grubunun Win32/KillDisk.NBB, Win32/KillDisk.NBC ve Win32/KillDisk.NBD Truva varyantları gibi yeni yıkıcı bileşenler kullandığını tespit etmiştir. Bu bileşenin asıl amacı rastgele verilerle dokümanları üzerine yazarak ve işletim sistemini önyükleme yapmasına engel olarak bilgisayar üzerindeki veri depolama yerine zarar vermektir [46].

```
unicode 0, <a.ivf.ivr.ivs.izz.izzy.jmv.jss.jts.jtv.k3g.kmv.lrec.lrv.l>
unicode 0, <sf.lsx.lvix.m15.m1pg.m1v.m21.m21.m2a.m2t.m2ts.m2v.m4e.m4u>
unicode 0, <.m4v.m75.mani.meta.mgv.mj2.mjp.mjpg.mk3d.mkv.mmv.mnv.mob.>
unicode 0, <mod.moff.moi.moov.mov.movie.mp21.mp21.mp2v.mp4.mp4.infovi>
unicode 0, <d.mp4v.mpe.mpeg.mpeg1.mpeg4.mpf.mpg.mpg2.mpgindex.mpl.mpl>
unicode 0, <s.mpsub.mpv.mpv2.mqv.msdvd.msh.mswmm.mts.mtv.mvb.mvc.mvd.>
unicode 0, <mve.mvex.mvp.mvy.mxf.mxv.mys.ncor.nsv.nut.nuv.nvc.ogm.ogv>
unicode 0, <.ogx.orv.otrkey.par.pds.pgi.photoshow.piv.pjs.playlist.pl>
unicode 0, <proj.pmf.pmv.ppj.prel.pro.pro4dvd.pro5dvd.proqc.prproj.pr>
```

Şekil 13.15. KillDisk.NBB tarafından tahrip etmek için hedeflenen dosya uzantılarının bir kısmının listesi [46]

İletişim firmalarına yönelik saldırılarda kullanılan Win32/KillDisk.NBB varyantı birçok doküman ve dosyayı tahrip etmek için kullanılmaktadır. Üzerine yazmaya ve silmeye çalıştığı uzun bir dosya uzantı listesi vardır. Varyantın

tam listesi 4000'den fazla dosya uzantısı içerir ve Şekil 13.15'te ilgili dosya uzantılarının bir kısmı gösterilmiştir.

Ukrayna'da enerji firmalarına yönelik gerçekleşen saldırılarda kullanılan KillDisk bileşeni biraz daha farklıdır. ESET'in analizlerine göre yeni versiyondaki değişiklikler:

- Tahrip yükü aktif olması gerektiğinde belirli bir zaman gecikmesini ayarlamak için komut satırı argümanını kabul eder.
- Windows olay loglarını siler: Uygulama, Güvenlik, Setup, Sistem
- Doküman silmeye daha az odaklıdır. Sadece 35 dosya uzantısı hedef alınmış olup ilgili uzantılar Şekil 13.16'da gösterilmiştir.

```
unicode 0, <.crt.bin.exe.db.dbf.pdf.djvu.doc.docx.xls.xlsx.jar.ppt.pp>
unicode 0, <tx.tib.vhd.iso.lib.mdb.accdb.sql.mdf.xml.rtf.ini.cfg.boot>
unicode 0, <.txt.rar.msi.zip.jpg.bmp.jpeg.tiff>,0
```

Şekil 13.16. KillDisk bileşeninin yeni varyantı tarafından tahrip etmek için hedeflenen dosya uzantıları listesi [46]

Sistemin önyükleme yapamaması için sistem dosyalarını silmesinin yanı sıra – Böyle tahrip edici trojan için tipik işlevselliği – özellikle endüstriyel sistemleri sabote etmek amacıyla elektrik dağıtım firmalarında tespit edilen KillDisk varyantı bazı ek işlevler içeriyor. Aktif duruma geldiğinde, KillDisk varyantı iki tane standart olmayan işlemi arar ve sona erdirir: komut.exe ve sec_service.exe.

Bu işlemlerden ikincisi (sec_service.exe) bir endüstriyel kontrol sisteminde kullanılan yazılımın (ASEM Ubiquity veya ELTIMA seri-ethernet konnektörü) kullandığı bir işlem ve zararlı yazılım bu uygulamanın çalışmasını engellemekle kalmayıp aynı zamanda rasgele verilerle çalıştırılabilir dosyanın üzerine yazmaktadır.

Bu işlemlerden birincisi (komut.exe) hakkında detaylı bir bilgi yoktur fakat Türkçede command yerine kullanılan komut anlamına gelmektedir. Bu durum Türkçe işletim sistemlerinin hedef alınabileceğini göstermektedir. Yukarıda açıklanan "build_id" değerlerinden "11131526trk" değerindeki "trk", "türk" olarak temsil edilmiş olabilir fakat "11131525" rakamlarının anlamları henüz anlaşılamamıştır. Stuxnet solucanındaki 19790509 değerindeki gibi İran-İsrail ilişkilerindeki gerilime manidar bir değer olup olamayacağı araştırmalarına devam edilecektir.

13.5. SONUÇ VE DEĞERLENDİRMELER

Bilgi güvenliğinin üç bileşeni gizlilik, bütünlük ve erişilebilirliktir. Bunlardan erişilebilirlik, SCADA sistemlerinin gerçek zamanlı çalışmasından dolayı en önemli bileşendir. Verilerin iletimi sırasında milisaniyeler seviyesinde bir zaman gecikmesinin bile fonksiyonel işlemlerin çok ciddi aksamalarına sebebiyet vermesi olasılığı yüksektir. Bu yüzden gerçek zamanlı çalışan SCADA sistemleri üzerinde güvenlik testlerinin yapılması sakıncalı olabilmektedir. Dolayısıyla SCADA sistemlerinin devreye alınmadan önce güvenlik testlerinin yapılması gerektiği sonucuna varılmıştır. Bu bağlamda, bazı özel sektör kuruluşlarının ve üniversitelerin SCADA sistemlerinin güvenliğine yönelik deney düzeneği ortamlarının var olduğu fakat ulusal çapta çalışmalar için yetersiz olduğu gözlemlenmiştir. Bu bakımdan ülkemizdeki ulusal enerji altyapısının güvenliğini sağlamaya yönelik ulusal bir araştırma geliştirme laboratuvarının ve deney düzeneklerinin kamu, üniversite ve özel sektör iş birliği ile oluşturulması gerektiği önerilmektedir.

Kritik bilgi sistemlerine yönelik risk değerlendirmeleri hayati derecede öneme sahip diğer bir unsurdur. Özellikle ülke güvenliğini ilgilendiren altyapılara yönelik siber saldırılar için risk değerlendirme teknikleri kullanılmalıdır. Bu bakımdan, Irmak ve Erkek'in [47] saldırı ağacı gösterimi ile çok nitelikli fayda teorisini kullanarak önerdikleri çalışma, kritik bilgi sistemlerinde risk değerlendirmesi için önemli bir rehberlik teşkil edebilir.

Genel bir sonuç olarak, fonksiyonel işlemlerini kaybetmesi, zarar görmesi veya veri iletiminde oluşan manipülasyonlar sonucunda toplum düzenini, insan hayatını, ekonomik kayıpları, ulusal veya global düzeyde güvenliği sekteye uğratabilecek kritik altyapı sistemlerinin güvenlik bilinciyle oluşturulması ve buna uygun tasarlanması gerektiği şüphesizdir. Kritik altyapılar içerisinde en önemli sistemlerden birisi olan SCADA sistemlerinin güvenliği hayati derecede öneme sahiptir. Bu sebeple özellikle ülkemizde elektrik dağıtım firmalarının kullandığı kontrol sistemlerinin haberleşme protokollerinin yeniden gözden geçirilmesi ve siber güvenlik açısından ele alınması gerekmektedir.

Teşekkür

Bu bölümde yer alan bilgiler ve çalışmalar, Prof. Dr. Erdal Irmak danışmanlığında İsmail Erkek tarafından hazırlanan "Modbus Temelli SCADA Sistemlerinin Siber Güvenliği için Yeni Bir Yaklaşım" adlı yüksek lisans tezinden derlenmiştir. Yazarlar, adı geçen tez çalışmasının yürütüldüğü Gazi Üniversitesi Fen Bilimleri Enstitüsü Bilgi Güvenliği Mühendisliği Ana Bilim Dalına teşekkürlerini sunar.

KAYNAKLAR

[1] Stouffer, K ., Falco, J. ve Kent, K. (2008). *Guide to Industrial Control Systems (ICS) Security Recommendations of the National Institute of Standards and Technology.* ***Nist Special Publication (800)82***.

[2] İnternet: Risk Based Security. Our New Year Vulnerability 'Trends' Prediction. URL: https://www.riskbasedsecurity.com/2015/12/our-new-year-vulnerability-trends-prediction/, Son Erişim Tarihi: 10.05.2017.

[3] Amanullah, M. T. O., Kalam, A. ve Zayegh, A. (2005). Network Security Vulnerabilities in SCADA and EMS. ***Proceedings of the IEEE Power Engineering Society Transmission and Distribution Conference***, 1–6, Dalian, Çin.

[4] İnternet: Idaho National Laboratory. Vulnerability Analysis of Energy Delivery Control Systems. URL: https://energy.gov/sites/prod/files/Vulnerability%20Analysis%20of%20Energy%20Delivery%20Control%20Systems%202011.pdf, Son Erişim Tarihi: 02.02.2017.

[5] İnternet: US Department of Homeland Security Centre for the Protection Of National Infrastructure. Cyber Security Assessments of Industrial Control Systems: Good Practice Guide. URL: https://www.ccn-cert.cni.es/publico/InfraestructurasCriticaspublico/CPNI-Guia-SCI.pdf, Son Erişim Tarihi: 17.04.2017.

[6] İnternet: Toolswatch Hackers Arsenal. ICS / SCADA Top 10 Most Dangerous Software Weaknesses. URL: http://www.toolswatch.org/wp-content/uploads/2015/11/ICSSCADA-Top-10-Most-Dangerous-Software-Weaknesses.pdf, Son Erişim Tarihi: 04.04.2017.

[7] Alves, R. ve Souza, A. (2014). A Summary of Control System Security Standards Activities in the Energy Sector. ***U.S. Department of Energy Office of Electricity Delivery and Energy Reliability***, sayı 1, 1–5.

[8] Zhu, B., Joseph, A. ve Sastry, S. (2011). A Taxonomy of Cyber Attacks on SCADA Systems. ***Proceedings - 2011 IEEE International Conferences on Internet of Things and Cyber, Physical and Social Computing, iThings/CPSCom 2011***, 380–388, Dalian, Çin.

[9] Eden, P., Blyth, A., Burnap, P., Cherdantseva, Y., Jones, K., Soulsby, H. ve Stoddart, K. (2015). A Forensic Taxonomy of SCADA Systems and Approach to Incident Response. ***Proceedings of the 3 International Symposium for ICS & SCADA Cyber Security Research***, 42–51, Ingolstadt, Almanya.

[10] Martin, B., Brown, M., Paller, A., Kirby, D. ve Christey, S. (2011). CWE - 2011 CWE/SANS Top 25 Most Dangerous Software Errors. ***MITRE***, versiyon 1.08.

[11] İnternet: Industrial Defender White Paper. Report from the Field : Seven Best Practices for Automation System Cyber Security and Compliance. URL: http://www.isssource.com/wp-content/uploads/2012/05/053012Industrial-Defender-Seven-Best-Practices.pdf, Son Erişim Tarihi: 10.06.2017.

[12] Nordlander, J. (2009). *What is Special About Scada System Cyber Security ? A Comparison between Existing Scada System Security What is Special about Scada System Cyber*. Doktora Tezi, Royal Institute of Technology, İsviçre.

[13] Graham, J. H. ve Patel, S. C. (2004). Security Considerations in SCADA Communication Protocols. ***Intelligent Systems Research Laboratory***, 502, 1–24.

[14] Huitsing, P., Chandia, R., Papa, M. ve Shenoi, S. (2008). Attack Taxonomies for The Modbus Protocols. ***International Journal of Critical Infrastructure Protection***, 1, 37–44.

[15] Irmak, E., Erkek, İ. (2018). Endüstriyel Kontrol Sistemleri ve SCADA Uygulamalarının Siber Güvenliği: Modbus TCP Protokolü Örneği. ***Gazi Üniversitesi Fen Bilimleri Dergisi Part C: Tasarım ve Teknoloji***, 6(1), 1-16.

[16] AlShemeili, A., Yeun, C. Y. ve Baek, J. (2016). PLC Monitoring and Protection for SCADA Framework. ***Advanced Multimedia and Ubiquitous Engineering***, 354, 259–267.

[17] Irmak, E., Erkek, I. ve Özçelik, M. M. (2017). Experimental Analysis of The Internal Attacks on Scada Systems. ***Gazi University Journal of Science***, *30*(4), 216-230.

[18] İnternet: Shodan. Shodan Search Engine. URL: https://www.shodan.io/, Son Erişim Tarihi: 16.05.2017.

[19] İnternet: Industrial Control Systems Cyber Emergency Response Team. Increasing Threat to Industrial Control Systems (Update A). URL: https://www.us-cert.gov/ics/alerts/ICS-ALERT-12-046-01A , Son Erişim Tarihi: 21.05.2017.

[20] Leverett, E. (2011). *Quantitatively Assessing and Visualising Industrial System Attack Surface*, Yüksek Lisans Tezi, Advanced Computer Science of University of Cambridge, Cambridge.

[21] İnternet: Tofino Industrial Security Solution. Project SHINE: 1,000,000 Internet-Connected SCADA and ICS Systems and Counting. URL: https://www.tofinosecurity.com/blog/project-shine-1000000-internet-connected-scada-and-ics-systems-and-counting, Son Erişim Tarihi: 21.05.2017.

[22] İnternet: Industrial Control Systems Cyber Emergency Response Team. ICS-CERT Monitor. URL: https://www.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Jul-Sep2013.pdf , Son Erişim Tarihi: 19:05.2017.

[23] İnternet: Wireshark. URL: https://www.wireshark.org/, Son Erişim Tarihi: 21.05.2017.

[24] İnternet: Nmap: the Network Mapper. URL: https://nmap.org/, Son Erişim Tarihi: 21.05.2017.

[25] İnternet: PLCSCAN, Google Code Archive - Long-term storage for Google Code Project Hosting. URL: https://code.google.com/archive/p/plcscan/, Son Erişim Tarihi: 21.05.2017.

[26] İnternet: SCADAhacker. Metasploit Modules for SCADA Vulnerabilities. URL: https://www.scadahacker.com/resources/msf-scada.html, Son Erişim Tarihi: 21.05.2017.

[27] İnternet: Rapid7. Modbusdetect. URL: https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/scanner/scada/modbusdetect.rb, Son Erişim Tarihi: 21.05.2017.

[28] İnternet: Rapid7. Modbusclient. URL: https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/scanner/scada/modbusclient.rb, Son Erişim Tarihi: 21.05.2017.

[29] İnternet: Modbus IDA. MODBUS Application Protocol. URL: http://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf, Son Erişim Tarihi: 10.03.2017

[30] İnternet: The Telegraph. CIA Plot Led to Huge Blast in Siberian Gas Pipeline - Telegraph. URL: https://www.telegraph.co.uk/news/worldnews/northamerica/usa/1455559/CIA-plot-led-to-huge-blast-in-Siberian-gas-pipeline.html, Son Erişim Tarihi: 21.05.2017.

[31] İnternet: Central Intelligence Agency. The Farewell Dossier. URL: https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol39no5/pdf/v39i5a14p.pdf, Son Erişim Tarihi: 21.05.2017.

[32] Turk, R. J. (2005). Cyber Incidents Involving Control Systems. ***US-CERT Control Systems Security Center***, 1–58.

[33] İnternet: BBC NEWS. Technology | Questions Cloud Cyber Crime Cases. URL: http://news.bbc.co.uk/2/hi/technology/3202116.stm, Son Erişim Tarihi: 21.05.2017.

[34] İnternet: ComputerWorld. Study: Slammer Was Fastest-Spreading Worm yet. URL: https://www.computerworld.com/article/2579971/study--slammer-was-fastest-spreading-worm-yet.html, Son Erişim Tarihi: 21.05.2017.

[35] Weiss, J. (2010). Protecting Industrial Control Systems from Electronic Threats, ABD: Momentum Press.

[36] İnternet: The Wall Street Journal. Electricity Grid in U.S. Penetrated By Spies. URL: https://www.wsj.com/articles/SB123914805204099085, Son Erişim Tarihi: 21.05.2017.

[37] E. Chien ve G. O'Gorman (2011). The Nitro Attacks: Stealing Secrets from the Chemical Industry. ***Symantec Security Response***, 1–8.

[38] İnternet: The Register Publication. Stuxnet 'A Game Changer for Malware Defence. URL: https://www.theregister.co.uk/2010/10/09/stuxnet_enisa_response, Son Erişim Tarihi: 21.05.2017.

[39] M. Knopová ve E. Knopová (2014). The Third World War? In The Cyberspace. Cyber Warfare in the Middle East. ***Acta Informatica Pragensia***, 3(1), 23–32.

[40] Chien, E., O'Murchu, L. ve Falliere, N. (2011). W32.Duqu The Precursor to the Next Stuxnet. ***Symantec Security Response***, 1(4), 1–71.

[41] Bronk, C. ve Ringas, E. (2013). Hack or Attack? Shamoon and the Evolution of Cyber Conflict. ***Institute for Public Policy Rice University***, 1–30.

[42] Fillinger, M. (2013). *Reconstructing the Cryptanalytic Attack behind the Flame Malware*. Yüksek Lisans Tezi, Institude for Logic, Language and Computation of Amsterdam University, Amsterdam.

[43] İnternet: The Washington Post. U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts. URL: https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html?utm_term=.f817d00970da, Son Erişim Tarihi: 21.05.2017.

[44] İnternet: ABC News. DHS: Hackers Mounting Organized Cyber Attack on U.S. Gas Pipelines. URL: https://abcnews.go.com/Blotter/dhs-hackers-mounting-organized-cyber-attack-us-gas/story?id=16304818, Son Erişim Tarihi: 21.05.2017

[45] İnternet: ESET Smart Security. ESET Finds Connection Between Cyber Espionage and Electricity Outage in Ukraine. URL: https://www.eset.com/int/about/newsroom/press-releases/research/eset-finds-connection-between-cyber-espionage-and-electricity-outage-in-ukraine/, Son Erişim Tarihi: 21.05.2017.

[46] İnternet: WeLiveSecurity | ESET. BlackEnergy by the SSHBearDoor: Attacks against Ukrainian News Media and Electric Industry. URL: https://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/, Son Erişim Tarihi: 21.05.2017.

[47] Irmak, E., Erkek, İ. (2016). Çok Nitelikli Fayda Teorisiyle Saldırgan Profiline Yeni Parametrelerin Eklenmesi. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, *2* (2), 1-9.

Bölüm 14

ISO/IEC 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİNDE KARŞILAŞILAN UYGULAMA ZORLUKLARI

Samime Meral - Halil İbrahim Bülbül

Son yıllarda bilgi güvenliğinin sağlanmasına yönelik birçok çalışma yapılmaktadır. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı bilgi güvenliğine yönelik yapılan çalışmalardan birisi olarak uluslararası düzeyde kabul görmüş bir standarttır. Söz konusu Standart aynı zamanda bir sertifikasyona sahiptir. Kuruluşlar Standarda göre oluşturduğu ve işlettiği Bilgi Güvenliği Yönetim Sistemini uluslararası akredite edilen kuruluşlar vasıtasıyla sertifikalandırabilmektedir. Standart ile Bilgi Güvenliği Yönetim Sistemleri, kuruluş tarafından karar verilen bir kapsam dâhilinde oluşturulmakta ve işletilmektedir. Kuruluşlar bu alanda danışmanlık veren firmalardan danışmanlık hizmeti alarak Bilgi Güvenliği Yönetim Sistemi için gerekli dokümantasyonu tamamlayıp oluşturulabilecekleri gibi kendi personeli ile de hiçbir danışmanlık almadan bu süreci kurup işletebilmektedir. Kuruluşların kendi personeli ile bu çalışmayı yürütmesi hâlinde, bizzat kuruluş personelinin ve kuruluşun sorumluluğunda olan bu sürecin çok iyi analiz edilerek tasarlanması ve uygulanması gerekmektedir. Kuruluş yapısı yeteri kadar analiz edilmeden ve Bilgi Güvenliği Yönetim Sistemi kapsamı doğru belirlenmeden süreci yürütmenin ve yönetmenin kuruluşlar için birçok zorluğa sebep olduğu değerlendirilmektedir. Kuruluşlar oluşturacakları Bilgi Güvenliği Yönetim Sistemi kapsamını belirlerken birtakım değerlendirme ölçütlerini dikkate almaktadırlar. Uygulanabilir ve etkin bir Bilgi Güvenliği Yönetim Sistemi için kuruluşların kapsam

belirleme çalışmasını titizlikle yapması gerekmektedir. Bir kuruluşta Bilgi Güvenliği Yönetim Sistemi kurulurken kuruluşun bütünü kapsama dâhil edilebileceği gibi, kuruluşun sadece belirli bir bölümü ya da hizmeti de kapsam dâhilinde tutulabilmektedir. Standart genel olarak kuruluşların bilgi varlıklarının güvenliğine odaklanmaktadır. Kuruluşlarda bilgi varlıklarının çoğunluğu genellikle Bilgi İşlem birimlerinde bulunmaktadır. Bu nedenle birçok kuruluş Bilgi Güvenliği Yönetim Sistemi kapsamını sadece bu birimlerle sınırlı tutmaktadır. Bazı kuruluşlar ise bilgi güvenliği hedeflerini daha yüksek tutmakta ve Bilgi Güvenliği Yönetim Sistemi kapsamını tüm kuruluş olarak belirlemektedir. Kapsamın bu şekilde geniş tutulması, kuruluşta bilgi güvenliğinin daha geniş boyutta ele alınmasını sağlarken, birçok uygulama zorluğunu da beraberinde getirmektedir. Bu bölümde, Bilgi Güvenliği Yönetim Sistemi (BGYS) kapsamının Bilgi İşlem birimine ek olarak kuruluşların diğer birimlerinin de dâhil edilecek şekilde belirlenmesinde karşılaşılan uygulama zorluklarının ortaya konulması ve Bilgi Güvenliği Yönetim Sistemini kendi personeli ile oluşturup yürütme kararı alan kuruluşlarda kapsam belirleme aşaması için konu ile ilgili farkındalık sağlanması amaçlanmaktadır.

14.1. GİRİŞ

Daha önceleri genellikle fiziksel ortamlarda tutulan bilgi, artık dijital ortamlara da taşınmıştır. Fiziksel ortamlarda tutulan bilginin korunması için fiziksel önlemlerin alınması yeterli olabilecekken, dijital ortamlarda muhafaza edilen bilginin korunması için fiziksel önlemlerin yanı sıra daha farklı önlemlerin alınması gerekmektedir.

Bilginin fiziksel ortamlardan dijital ortamlara geçmesi ile, bilginin korunmasının yanı sıra bilgi güvenliği kavramı önemli hâle gelmiştir. Geçmişte sadece fiziksel güvenliğin tesis edilmesi ile sağlanan bilgi güvenliği, günümüzde kurumların en çok zorlandıkları ihtiyaçların başında gelmektedir [17].

Bilgi güvenliği unsurları genel kabul görmüş hâliyle gizlilik, bütünlük ve erişilebilirlik diğer bir ifadeyle kullanılabilirlik olarak değerlendirilmektedir. Buna göre bilgi güvenliği konuları incelenirken, Şekil 14.1'de yer aldığı gibi üç temel bakış açısı dikkate alınır [16]:

Şekil 14.1. Gizlilik-Bütünlük-Erişilebilirlik

Gizlilik; önemli ve hassas bilgilerin istenmeyen biçimde yetkisiz kişilerin eline geçmesi önlenmesi ve sadece erişim yetkisi verilmiş kişilerce erişilebilir olduğu garanti altına alınması, **bütünlük**; bilginin bir kısmının veya tümünün yetkili olmayan kişilerce değiştirilmesinin, silinmesinin ve bozulmasının önlenmesi, **erişilebilirlik**; bilgi veya bilgi sistemlerinin sürekli kullanıma hazır ve erişilebilir olması şeklinde tanımlanmaktadır [1]. Bunlar genel kabul görmüş bilgi güvenliği unsurları olarak değerlendirilirken, bazı çalışmalarda bu unsurlara destek olan ilkelerden de bahsedilmektedir. Örneğin bir çalışmada [2], belirli bir eylemin gerçekleştirilmesinden kimin ya da neyin sorumlu olduğunun belirlenmesi olarak sorumluluk ilkesinin bilgi güvenliğine katkı sağlayan bir ilke olduğundan bahsedilmektedir. Bunların dışında erişim denetimi, güvenilirlik ve emniyet etkenleri de bilgi güvenliğini destekleyen unsurlardır [14]. Özetle, sistemlerin sağlıklı bir şekilde işleyebilmesi ve kullanıcılarına eksiksiz hizmet verebilmesi açısından gizlilik, bütünlük ve erişilebilirlik kavramlarının korunması gerekmektedir [21].

Bilgi güvenliğinin gizlilik, bütünlük ve erişilebilirlik unsurlarına sahip olduğunu ifade eden bir çalışma da ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı çalışmasıdır. Standart, ISO (Uluslararası Standardizasyon Kuruluşu) tarafından yayımlanmıştır. ISO/IEC 27001 Standardı bilgi güvenliği alanında dünya çapında genel kabul görmüş bir standarttır [3]. Bu eserde detaylı olarak açıklanan bu standart, bir BGYS'nin kurulması, uygulanması, sürdürülmesi ve

sürekli iyileştirilmesi için şartları ortaya koymak amacıyla hazırlanmıştır [4]. Standardın uygulanması ve BGYS süreçlerinin iyi şekilde işletilmesine yönelik birçok çalışma bulunmaktadır. Standart süreçlerine uygunluğun değerlendirilmesine yönelik yazılımlar da mevcuttur [5]. Standardın bir kuruluşta uygulanarak BGYS'nin kurulması sonucu sertifikanın alınması, kuruluşun bilgi güvenliğini bir düzen içerisinde icra etmesini sağlamaktadır. Uluslararası kabul görmüş olan Standart, ister kamu ister özel olsun, her ölçekteki kuruluşa uygun, etkili bir güvenlik yönetim sisteminin gerekliliklerini ortaya koymaktadır [6].

Kuruluşlar sahip oldukları bilgi varlıklarına ilişkin olası risk ve tehditleri belirlemek kurumsal bilgi güvenliğini sağlamak için her türlü tedbiri almak adına birtakım çalışmalar yürütmektedir. Kurumsal bilgi güvenliği, sistem, teknoloji, insan, eğitim gibi pek çok faktörü tek çatı altında toplayarak yönetilmesi zor bir süreçtir [18]. Kuruluşlar, bu standart kapsamında sertifika alabilmek için bilgi güvenliğinin sağlanmasına yönelik standart metninde belirtildiği şekilde BGYS süreçlerini oluşturmaktadır.

BGYS'nin kurulmasıyla; olası risk ve tehditlerin tespit edilmesi, güvenlik politikalarının oluşturulması, denetimlerin ve uygulamaların kontrolü, uygun yöntemlerin geliştirilmesi, örgütsel yapılar kurulması ve yazılım/donanım fonksiyonlarının sağlanması gibi bir dizi denetimin birbirini tamamlayacak şekilde gerçekleştirileceği ifade edilmektedir [13]. BGYS'nin kurulması bir kuruluş için stratejik bir karardır. Bu nedenle; kuruluşun ihtiyaçlarına uygun olarak ölçeklenmesi ve güncellenmesi ile sorunsuz bir şekilde kuruluşa entegre edilmesi gerekir [19]. BGYS süreçleri kuruluşların belirlediği kapsam dâhilinde oluşturulmakta ve işletilmektedir. Bir kuruluşta BGYS'nin kurulması ve sürdürülmesi; kuruluşun sahip olduğu personel sayısı, hedefleri, iş süreçleri, güvenlik gereksinimleri ve yapısından etkilenmektedir. Gerek kamu gerek ise özel sektör kuruluşları, BGYS süreçlerini kurmak ve etkin bir şekilde sürdürülebilirliğini sağlamak için sahip oldukları yapıyı iyi analiz ederek BGYS'yi kurup işletecekleri kapsamı doğru bir şekilde belirlemelidir. Kuruluşların kendi personeli ile oluşturup sürdürmeyi düşündükleri bu sürecin etkin ve uygulanabilir olması için kuruluşun büyüklüğünün, sahip olduğu bilgi varlıklarının, bu süreci yürütecek ve yönetecek personelin sayısı ve niteliğinin, kuruluşun sahip olduğu bilgi teknolojileri alt yapısının, kuruluşun tüm paydaşlarının beklentilerinin ve bilgi güvenliği ihtiyaçlarının değerlendirilmesi gerekmektedir. İlgili parametreler iyi analiz edilmeden BGYS kapsamının geniş tutularak çalışmaların yürütülmesi kuruluşlar ve kuruluşta süreci yöneten personel için birçok zorluğu beraberinde getirmektedir.

Bu bölümde, kuruluşta BGYS kapsamının dar veya geniş tutulduğu durumlarda karşılaşılan zorluklar üzerinde durulmuştur. Öncelikle BGYS kurulumu ve işletiminde yapılması gereken çalışmalardan genel olarak bahsedilmektedir, daha sonra BGYS kapsamının geniş tutulmasının, dar tutulmasına göre hangi zorlukları beraberinde getirdiği anlatılmaktadır.

14.2. BGYS KAPSAMINDA YAPILMASI GEREKEN ÇALIŞMALAR

Öncede bahsedildiği gibi BGYS kurulumunun ilk aşaması kapsamın belirlenmesidir. Bir kuruluşta BGYS kurulurken kuruluşun bütünü BGYS kapsamına dâhil edilebileceği gibi, kuruluşun sadece belirli bir bölümü ya da hizmeti de kapsamda tutulabilir. Kapsamın geniş ya da dar tutulması kararını, üst yönetimin bilgi güvenliği konusundaki hedefleri belirlemektedir. BGYS kapsamı yazılı olarak muhafaza edilmektedir.

BGYS'nin temel yapısını açıklayan Bilgi Güvenliği Politikası oluşturulmaktadır. Bilgi Güvenliği Politikası, BGYS'nin kuruluşta uygulanmasında, kuruluşun amaçlarına uygun bilgi güvenliğine ilişkin genel hedefleri ortaya koyan bir metindir.

Kuruluşun bilgi güvenliği hedeflerine yönelik olarak hazırlanan Bilgi Güvenliği Politikası'nı destekleyen diğer yardımcı politikalar oluşturulmaktadır. Bilgi Güvenliği Politikası kurumsal bilgi güvenliği ana hedeflerini ortaya koyarken, diğer politikalar Bilgi Güvenliği Politikası'nın amaçlarına hizmet etmektedir.

Bilgi Güvenliği Politikası ve diğer politikalarda yer alan hükümlerin uygulanmasına yönelik yol gösterici nitelikte olan prosedürler oluşturulmaktadır. Söz konusu prosedürler, kurumsal iş süreçlerinin gerçekleştirmesinde işlem adımlarını ortaya koymaktadır. İş süreçlerinin gerçekleştirilmesinde hangi prosedürlerin uygulanacağı ilgili politika metninde belirtilmektedir. Ayrıca bilgi güvenliği politikasında kurumun, çalışanların ve kurumla ilişkili tüm paydaşların görev ve sorumluluğu ve sorumluluğun nasıl tesis edileceğine dair bilgiler yer almaktadır. Bilgi güvenliği politikası aşağıdaki ihtiyaçları güvenceye alır;

- Süreçler ve bilgi varlıklarının tanımlanması ve bunlarla ilgili risk değerlendirmelerinin metodolojik olarak gerçekleşmesi,
- Bilginin yetkisiz erişimden korunması,
- Bilginin gizliliğinin sağlanması,
- Bilginin bütünlüğünün korunması,

- İş süreçlerinin ihtiyaç duyduğu her anda bilgiye erişimin mümkün olması,
- Yasal yükümlülüklerin ve sözleşmelerden doğan hukuki yükümlülüklerin yerine getirilmesi,
- İş sürekliliği planlarının geliştirilmesi ve iyileştirilmesi,
- Tüm personele Bilgi Güvenliği Farkındalık eğitimlerinin sağlanması,
- Tüm Bilgi Güvenliği ihlallerinin veya ihlal şüphesinin Bilgi Güvenliği Yönetim Kurulu'na bildirilmesini ve incelenmesinin sağlanması.

Kurumsal iş süreçleri prosedürlere uygun şekilde gerçekleştirilirken, iş sürecinin gerçekleştirilmesine yönelik kayıtların tutulması için formlar kullanılmaktadır. Formlar, her bir prosedürün ne şekilde uygulandığına yönelik bilgiler içermektedir.

BGYS kapsamında;

- Kurumsal iş süreçlerinin etkin bir şekilde işletilmesi için politika, prosedür ve formların yanı sıra liste, kılavuz, plan, taahhütname, sözleşme, rapor vb. yardımcı dokümanlar da oluşturulmaktadır. İlgili dokümanlar birbirlerine atıflarda bulunarak bütünlük elde edilmektedir.
- Dokümanda bulunan tüm hususlar kuruluş yönetimi tarafından onaylanmakta ve personele duyurulmaktadır.
- Kuruluş üst yönetimi, BGYS'nin kurulması, işletilmesi ve sürekli iyileştirilmesi için ilgili kişilere rol ve sorumluluk atamaları yaparak BGYS organizasyon yapısını oluşturmaktadır.
- Organizasyon yapısında yer alan kişilerin bilgi güvenliği alanında yetkinlik seviyelerinin arttırılması ve BGYS süreçleri hakkında bilgi edinmeleri amacıyla eğitimler düzenlenmektedir.
- Organizasyon yapısının ve BGYS kapsamında oluşturulan dokümanlarının tanıtımları ile personelin bilgi güvenliği alanında bilinçlenmeleri için Bilgi Güvenliği Farkındalık eğitimleri düzenlenmektedir.
- Kuruluş bilgi varlıklarının yer aldığı varlık envanteri oluşturulmaktadır. Varlık envanterinde; bilgi varlıklarının türü, kategorisi, sahibi, operasyonel sahibi, bulunduğu yer ve gizlilik, bütünlük ve erişilebilirlik dereceleri gibi bilgiler yer alır.
- Bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik dereceleri baz alınarak önem dereceleri ortaya konulmaktadır.

- Varlık envanterinde yer alan bilgi varlıklarının üzerinde risk değerlendirme çalışmaları gerçekleştirilmektedir. Risk envanteri oluşturulmaktadır. Risk envanterinde, her bir bilgi varlığının maruz kalabileceği risklere ilişkin bilgiler bulunmaktadır. Envanterde yer alan risklerin gerçekleşme olasılıkları, varlığın önem derecesiyle birlikte değerlendirilerek varlıkların risk dereceleri belirlenmektedir. Risk değerlendirme ile ilgili birçok metot bulunmaktadır. Bu konuda yapılan bir çalışma [7] risk değerlendirme için bir yöntem sunmaktadır. Risk envanterinde yer alan riskleri ortadan kaldırmak veya etkisini en aza indirmek için uygulanması gereken kontroller belirlenmekte ve uygulanmaktadır.

Belirlenen kontrollerin uygulanıp uygulanmadığının teyit edilmesi için kuruluşta iç tetkik çalışmaları gerçekleştirilerek tetkik sonuçları rapora bağlanmaktadır. İç tetkik çalışmaları neticesinde tespit edilen uygunsuzlukların giderilmesi ve tekrarının önlenmesi amacıyla uygulanacak yöntemlerin belirlendiği düzeltici ve iyileştirici faaliyetler belirlenmektedir.

Gerçekleştirilen tüm çalışmalar neticesinde risk derecesi kuruluşun belirlemiş olduğu risk yönetim prosedürüne göre yüksek olarak belirlenen riskler yönetim tarafından değerlendirilerek riskin ortadan kaldırılması veya azaltılması amacıyla alınabilecek önlemler belirlenmektedir. Önlem alınamayan ve kuruluşun belirlemiş olduğu risk yönetim prosedürüne göre artık risk olarak kabul edilen riskler yönetim tarafından kabul edilmektedir.

14.3. BGYS KAPSAMINDA GENİŞ TUTULMASINDAKİ UYGULAMA ZORLUKLARI

BGYS kurumun hassas bilgilerini yönetebilmek amacıyla benimsenen sistematik bir yaklaşımdır [14]. BGYS'de, bilgi ve veri, yazılım, sistem, fiziksel, personel ve soyut varlıklar gibi bilgi varlıklarına yönelik güvenlik üzerine odaklanılmaktadır. Son zamanlarda bilgi varlıklarının çoğunlukla bilgi sistemleri üzerinde tutulması nedeniyle, BGYS genellikle kuruluşların Bilgi İşlem birimleri temel alınarak kurulmaktadır. Bazı durumlarda sadece Bilgi İşlem birimleri kapsamında da BGYS kurulabilmektedir. Kapsamın geniş ya da dar tutulması genellikle üst yönetimin bilgi güvenliği konusundaki hedefleri ile ilişkilidir. Ancak yapılan bir çalışma [9] kurumsal bilgi güvenliğinin

sağlanması noktasında BGYS ile ilgili yanlış algılamalardan ve olması gerekenlerden bahsederek, BGYS'nin kurumun tüm birimlerini kapsayan ve iş süreçleri ile ilişkili olan bir bilgi güvenliği projesi olduğunu ifade etmektedir.

Standart, BGYS'nin tüm kuruluşu kapsayıp kapsamaması konusunda bir zorunluluk getirmemektedir. Ancak kuruluşlar BGYS kapsamına dâhil etmeyeceği birimlere karar verirken kapsama dâhil etmeme nedenlerini net şekilde ortaya koyabilmelidir. Kapsam belirlenirken nedenleri açık bir şekilde ortaya konulması hâlinde kuruluşun bazı birimleri kapsamda değerlendirilebilecekken, bazı birimler kapsam dâhiline alınmayabilmektedir. Benzer şekilde kuruluşun sadece belirli hizmetlerini dâhil edecek şekilde de kapsam daraltılabilir. Kuruluş bu süreci danışmanlık hizmeti almadan kendi personeli ile yürütüp yönetecek ise bu noktada önemli olan kuruluşun yapısı, büyüklüğü, iş süreçleri, bilgi güvenliği hedefleri, kurumsal bilgi teknolojileri yapısı ve tüm bu süreci yürütüp yönetecek personel sayısı ve niteliğidir. Nispeten personel sayısının, birimleşmenin ve bilgi varlıklarının daha fazla olduğu ve bilgi teknolojileri birimlerinin iyi organize edilmediği kuruluşlarda, kuruluş personeli ile BGYS çalışmalarının yürütülmesinde zorluklarla karşılaşılabilmektedir.

BGYS kapsamı olarak sadece Bilgi İşlem birimi belirlendiği durumlarda BGYS kurulumunda ana odak noktası söz konusu birim olacakken, bilgi güvenliği konusunda ilişkili oldukları birimlerde de ilişkide oldukları konu hakkında BGYS ile ilgili çalışmaların yapılması gerekmektedir. BGYS'nin sertifikalandırılması sürecinde de bu konu dikkate alınmaktadır. Uluslararası akredite olan bir sertifikalandırma kuruluşu tarafından sertifikalandırma denetimi ve sertifika alındıktan sonra devamlılığının sağlanıp sağlanmadığının kontrolü olan gözetim denetimi için kuruluş tarafından BGYS kapsamına alınan tüm birimlerde denetim faaliyeti gerçekleştirilmektedir. Bu doğrultuda kuruluş tarafından belirlenmiş olan BGYS kapsamı, sertifikanın alınması ve alındıktan sonra sürekliliğinin sağlanması noktasında da yapılacak çalışmalar için önem arz etmektedir.

BGYS kapsamının tüm kuruluş olarak belirlenmesi; kuruluşun bilgi güvenliği anlamında ciddi oranda güvende olmasını sağlayabilecekken, BGYS kuruluşu ve işletiminde ciddi oranda çalışma yapılmasını gerektirecektir. Kapsamın sadece Bilgi İşlem birimi olarak belirlendiği durumlarda ise; bu birimde bulunan bilgi varlıklarının güvenliğinin sağlanmasına yönelik Standartta yer alan çalışmalar yapılacakken, diğer birimlerde bulunan bilgi varlıklarının güvenliği üzerinde Standartta belirtilen çalışmalar yapılmayacaktır. Oysa, Bilgi

İşlem birimleri haricindeki İnsan Kaynakları, Hukuk, İdari Mali İşler gibi birimlerde de kuruluşa ait ciddi güvenlik seviyesinin arttırılması gereken bilgi varlıkları var olabilmektedir. BGYS'de temel olan kuruluş bilgi varlıklarının belirlenmesi, bilgi varlıklarına yönelik risklerin tespit edilmesi, kapsam dâhilindeki birimlerde iç tetkik faaliyetlerinin gerçekleştirilmesi ve sonuçların rapora bağlanması, tespit edilen uygunsuzluklar için düzeltici iyileştirici faaliyetlerin belirlenip sürekli olarak takibinin yapılması, tespit edilen risklerin üst yönetime sunulması ve alınan kararların uygulamaya konulmasıdır. Tüm bu süreç; devamlılığı sağlanması gereken ve belirli zaman aralığında sistematik olarak ilerleyen bir süreçtir.

BGYS kapsamının geniş tutulup tüm kuruluş birimlerinin çalışmalara dâhil edildiği durumlarda; kuruluşta BGYS çalışmalarının yürütülmesi ve yönetilmesi için oluşturulan BGYS organizasyon yapısında yer alan BGYS Üst Yönetim, BGYS Üst Yönetim Temsilcisi, BGYS Yöneticisi ve BGYS Birim Sorumluları gibi rollere kuruluş personelinden oluşan, konu ile ilgili yeteri kadar bilgisi ve farkındalığı olmayan kişiler atanabilmektedir. Bu nedenle; kuruluşun kendi personeli ile yürüteceği BGYS'nin kapsamının geniş tutulması, kapsamın dar tutulmasına göre daha fazla iş yükü gerektirmesinin yanı sıra başkaca uygulama zorluklarının meydana gelmesine de neden olabilmektedir. Bunlar;

Bilgi Güvenliği Farkındalığı

- Bilgi İşlem birimlerinde görevli olan personel genellikle görev tanımları gereği bilgi varlıklarının güvenliği konusunda belirli oranda bilgiye sahiptirler. Gerek almış oldukları eğitimler, gerekse mesleğini icra ederken karşılaştıkları olumsuz durumlar Bilgi İşlem personelinin bilgi güvenliği konusunda farkındalık seviyelerinin artmasına yardımcı olmaktadır. Bilgi İşlem unsurları olan yazılım, sistem, ağ, veri tabanı vb. tüm konularda bilgi güvenliği ayrı ayrı önemli bir husus olarak değerlendirilmektedir.
- Bilgi İşlem haricinde bir birimde görev alan kişiler, genellikle yaptığı ve yöneldiği çalışma alanı itibarıyla bilgi sistemleri konusundan uzak kalan kişiler olup, bu kişilerin bilgi güvenliği konusunda bilgi ve farkındalık düzeyleri yeterli seviyede olmamaktadır.
- Kuruluşta görevli kişilerin bilgi güvenliği konusundaki bilgi ve farkındalık düzeylerine bağlı olarak, BGYS kapsamının sadece Bilgi İşlem birimi olarak belirlendiği durumlarda sistemin kurulması ve

işletilmesi, BGYS kapsamına diğer birimlerin de dâhil edilmesi durumuna göre daha kolay olabilmektedir. Çünkü BGYS kurulumunda üzerinde durulan en önemli noktalardan birisi, kişilerin bilgi güvenliği konusunda bilgi ve farkındalık düzeylerinin arttırılması hususudur. Bu konu için belirli dönemlerde farkındalık konusunda eğitimlerin verilmesi gerekmektedir. Kişilerin yeterli bilgi güvenliği farkındalığına erişmesi hâlinde BGYS süreçlerinin kurulması ve işletilmesi bir hayli kolay olacaktır. Çünkü kişiler, bilgi varlıklarını kullanırken bilgi güvenliği konusunda daha dikkatli davranacak ve bu sayede bilgi güvenliği sağlanması hususunda önemli bir adım atılmış olacaktır.

BGYS Organizasyon Yapısı

- BGYS kapsamına sadece Bilgi İşlem biriminin alındığı durumlarda BGYS organizasyon yapısı da genellikle bu birimde görev yapan yönetici ve personelden oluşmaktadır. Personelin bilgi güvenliği konusundaki bilgi ve farkındalık düzeylerine benzer şekilde BGYS organizasyon yapısında yer alan kişilerin bilgi ve farkındalık düzeylerinin yüksek oluşu da süreçlerin oluşturulması ve işletilmesi konusunda kolaylık sağlayabilmektedir.
- Kapsama tüm birimlerin dâhil edilmesi hâlinde organizasyon yapısında Bilgi İşlem birimi yöneticisi ve personelinin dışında kişiler de yer alacaktır. Personelin bilgi güvenliği konusundaki bilgi ve farkındalık düzeylerinin düşük oluşunda konu bireysel sıkıntıların giderilmesiyle çözümlenebilecek iken; üst yönetimin bilgi ve farkındalık düzeylerinin düşük oluşu, kuruluşun bilgi güvenliği konusundaki hedeflerini bile değiştirebilecek nitelikte olabilmektedir. Bu durumlarda kişilerin ikna edilmesi konusunda birtakım zorluklarla karşılaşılabilmektedir. BGYS kurulumunun her aşamasında ilgili belgeler için yönetimden onay alınması gerektiğinden, bu aşamada konuların gerekliliğinin ve nedenlerinin sürekli olarak yönetimdeki kişilere detaylı olarak izah edilmesi gerekmektedir. BGYS kurulumu ve işletilmesinde kuruluşun üst yönetiminin bu konuya değer vermesi ve desteklemesi süreci kolaylaştırabilecekken, konuyu yeteri kadar önemsememesi ve desteğini hissettirmemesi süreci ciddi oranda zorlaştıracaktır.

Varlık ve Risk Envanterleri

- Varlık kuruluş için değeri olan ve korunması gereken her şeydir [20]. BGYS kapsamı belirlendikten sonra varlık envanteri çıkarılır ve risk değerlendirmesi varlıklar üzerinden gerçekleştirilir. BGYS kapsamı geniş tutulduğu durumlarda, kapsamda yer alan tüm birimlerde BGYS süreçlerinde görevli kişilerin varlık envanterinin güncel tutulması konusunda yeterli özeni göstermesi genellikle daha zordur. Kuruluşta birimler arası personel sirkülasyonun çok olduğu ve varlık envanterinin manuel takibinin yapıldığı durumlarda, birimlere ait varlık envanterlerinin güncelliğinin sağlanması bir hayli zorlaşmakta ve personelin inisiyatifine kalacak hâle gelebilmektedir. Söz konusu birimlerde çalışan personelin varlık envanterinin güncel tutulmasında ihmalci davranışları çok ciddi yeni risklerin ortaya çıkmasına neden olabilmektedir. Dolayısıyla bilgi varlıklarına göre belirlenen risk envanteri de güncelliğini yitirebilmektedir. Bazen kişiler bu ihmalden ziyade konunun önemli olmadığını düşünerek kötü niyet barındırmadan varlık ve risk envanterinin güncelleştirilmemesine neden olabilir. Ancak kişilerin birimleri nezdinde önemsiz olarak yorumladığı konular, BGYS bir bütün olarak değerlendirildiğinde çok önemli olabilmektedir. BGYS'nin bütünsel olarak değerlendirilebilmesi için ise kapsama dâhil edilen tüm birimlere ilişkin süreçlerin entegre bir şekilde çalışması gereklidir. Bunun için BGYS süreçlerinde yer alacak organizasyon yapısındaki kişilerin gerekli sayı ve işin gerektirdiği nitelikte olması gereklidir. Tüm kişilerin BGYS süreçlerinde yeterli özeni göstermesi durumunda, süreçlerin entegrasyonu sağlanarak BGYS hedeflerine daha iyi şekilde ulaşılabilecektir.

Bürokratik Engeller

- Meydana gelen en önemli zorluklardan birisi de bürokrasidir. Kapsamın geniş tutulmasıyla, BGYS organizasyon yapısının yanı sıra sürecin oluşturulması ve işletilmesinde birçok farklı birimden kişiler görevli olacaklardır. Kapsamın Bilgi İşlem birimi olarak daraltıldığı durumlarda kişilerin tek bir paydada buluşabilmesinin daha kolay olması muhtemeldir. Çünkü BGYS kapsamında yer alan bilgi güvenliğine ilişkin konular genel olarak çoğunluk tarafından kabul görmüş konulardır. Ancak farklı alan ve mesleklerden kişilerin bilgi güvenliği konusunda bir paydada buluşabilmesi zor olabilmektedir.

- BGYS'nin Bilgi İşlem birimi haricindeki birimlerde de işletilmesi gerektiğinden ilgili birimlerin yöneticilerinin de konuya dâhil olması ve birimi ile ilgili konularda gerekli onayları vermesi gerekmektedir. Ancak söz konusu birim yöneticilerinin BGYS süreçlerini, organizasyon yapısında görev yapan kişiler kadar bilemediğinden, birimi dâhilinde değerlendirilen bilgi güvenliği konularını kendisine yöneltilen birer tehdit olarak algılayabilmektedir. Bunun sonucu olarak da ilgili belgelerin onaylanması ve sürecin devamlılığının sağlanması konusunda zorluklar çıkabilmektedir. Kapsama dâhil edilen her birim yöneticisinin bu şekilde konuyu anlaması için geçen zaman dikkate alındığında bürokratik engellerin BGYS süreçlerini ne denli etkilediği ortaya çıkmaktadır.
- BGYS süreçlerinin oluşturulması ve işletilmesinde kuruluşta görevli tüm personele birtakım görevler düşeceğinden, personelin yapması gerekeni aynı özende ve bitirmesi gereken zamanda yapamaması veya yapmaması, birim yöneticilerinin yanı sıra, birimlerde görevli personel içinde bir bürokratik engel oluşturabilmektedir. Aynı şekilde bürokratik engellerde en fazla role sahip olanlardan birisi de organizasyon yapısında yer alan kişilerdir. Bu kişiler de BGYS süreçlerinin kurulması ve işletilmesinde işlerin aksamasına neden olacak tavırlar sergileyebilmektedir. Dolayısıyla; gerek organizasyon yapısında yer alan kişiler, gerekse birimlerde görevli olan kişi ve yöneticiler BGYS'nin kapsamının geniş tutulmasında bürokratik engellerin oluşmasına neden olabilmektedirler. Kapsama dâhil edilen birim ve hizmet sayısı arttıkça, süreçte görev alacak kişi sayısının artmasına bağlı olarak bürokratik engellerin artacağından bahsedilebilir.

İş Süreçlerinin Entegrasyonu

- BGYS süreçlerinin uygulanmasındaki zorluklardan bir diğeri de iş süreçlerinin entegrasyonunda meydana gelen birtakım zorluklardır. Kuruluşların sahip oldukları bilgi varlıkları sürekli değişiklik gösterdiğinden, kuruluş içerisindeki bilgi güvenliği konusundaki riskler de sürekli değişmektedir. Tüm bunların takibinin sağlıklı bir şekilde yapılabilmesi için tüm süreçlerin entegre bir şekilde ele alınması gerekmektedir.
- BGYS kapsamının sadece Bilgi İşlem birimi olarak belirlendiği durumlarda süreçlerin entegre edilmesi daha kolaydır. BGYS ilkelerin-

den biri olan görevler ayrılığı prensibine bağlı olarak, tüm personel görevleri ile ilgili ortaya çıkan ya da değişiklik gösteren bilgi varlıkları konusunda ilgili bilgi varlığının varlık envanterine eklenmesi ya da değiştirilmesi hususunda gerekli bilgilendirmeleri yapacaktır. Bu sayede Bilgi İşlem birimi dâhilinde ortaya çıkan yeni risklerin risk envanterinde yer alması sağlanmış olacaktır.

İç Tetkik Süreci

- BGYS süreçlerinin en önemlilerinden birisi iç tetkik sürecidir. İç tetkik, iç tetkik eğitimini başarıyla tamamlayan kuruluş personeli tarafından gerçekleştirilir. Söz konusu eğitimler genelde bilgi sistemleri konusunda genel bilgilere sahip olmaları bakımından Bilgi İşlem personeli tarafından daha kolay bir şekilde geçilebilmektedir. Genel bilgi sistemleri bilgi seviyesi düşük olan personel bu eğitimlerde biraz daha zorlanabilmektedir. BGYS kapsamının Bilgi İşlem birimi ile dar tutulduğu durumlarda bu eğitimleri alan kişi sayısı az olacağından eğitimin daha etkili olabileceği değerlendirilebilir. Ayrıca Bilgi İşlem personeli haricindeki personelin gerçekleştireceği iç tetkik faaliyetinin etkinliği de sorgulanmalıdır.
- Kapsamın geniş tutulduğu durumlarda iç tetkikleri gerçekleştiren tetkikçiler konuları farklı biçimlerde ele alabilirler. Tetkiklerin farklı şekilde ele alınması sonucu tetkik raporları da farklı formatlarda olabilmektedir. Bu konuda da tüm iç tetkikçilerin tek bir paydada buluşabilmesi genelde zordur. Aynı şekilde birimlerin görev alanlarına göre farklı iş süreçlerinin varlığı da iç tetkik süreçlerini zorlaştırmaktadır.

Düzeltici ve İyileştirici Faaliyetlerin Takibi

- İç tetkik faaliyeti sonrasında tespit edilen uygunsuzluklara ilişkin düzeltici ve iyileştirici faaliyetler tanımlanmaktadır. Kapsamın dar tutulduğu ve sadece Bilgi İşlem birimi personeli ve yöneticisinin aktif olarak yer aldığı durumda; tanımlanan düzeltici ve iyileştirici faaliyetlerin takibinin yapılması, söz konusu faaliyet için aksiyon sorumlularının atanması, uygunsuzluğun durumunun sürekli takip edilmesi, uygunsuzluğun kapatılması ve imza/onay süreçlerinin yürütülmesi hem çok daha kolay hem de zamandan tasarruf sağlamak ve tespit edilen uygunsuzluk kuruluş için büyük bir tehdide dönüşmeden önlem almak adına çok önemlidir.

Yönetimin Gözden Geçirme Toplantıları

- BGYS kapsamında gerçekleştirilen tüm çalışmalar neticesinde risk derecesi kuruluşun belirlemiş olduğu risk yönetim prosedürüne göre yüksek olarak belirlenen riskler yönetimin gözden geçirme toplantısında değerlendirmek üzere üst yönetime sunulmaktadır. Üst yönetim tarafından değerlendirme yapılarak tespit edilen riskin ortadan kaldırılması veya azaltılması amacıyla alınabilecek önlemler belirlenmektedir. Kapsamın geniş tutulduğu durumda BGYS organizasyon yapısında tanımlı olan üst yönetim rollerinde Bilgi İşlem birimi haricindeki diğer birim personeli ve yöneticileri yer alacağı için yönetimin gözden geçirme toplantılarını organize etmek, şeffaf ve objektif bir şekilde mevcut durumu paylaşmak ve tartışmak, etkili kararlar alabilmek zorlaşmaktadır.

Diğer Nedenler

Bilgi İşlem birimlerinin organizasyonuna yönelik literatüre geçmiş birçok çalışma bulunmaktadır. Bilgi İşlem birimlerinin organize edilmesi genellikle literatüre geçmiş çalışmalar baz alınarak gerçekleştirilmektedir. ISACA (Information Systems Audit and Control Association) ve ITGI (IT Governance Institute) tarafından yayımlanan COBIT 5 (Bilgi ve İlgili Teknolojiler için Kontrol Hedefleri) çerçevesi bu çalışmalara bir örnek olarak verilebilir. Bu tip çerçeve modellerin uygulandığı kuruluşlarda BGYS süreçlerinin uygulanması bazı kolaylıklar sağlayabilmektedir. Ancak birlikte uygulanmasının bazı dezavantajları da olabilmektedir [8]. Bu tip modellerle ilgili birçok çalışma örneği bulunduğundan kuruluşta uygulanan bilgi sistemleri organizasyon yapısı ile ilgili birçok bilgi birikimine sahip olunması mümkün olabilmektedir. Bu bilgi birikimi ile genel kabul görmüş kurallar Bilgi İşlem birimlerince kolaylıkla uygulanabilmektedir. Kuruluşlarda bulunan diğer birimler, genellikle belirli bir odak noktasında toplanamadığından Bilgi İşlem birimleri kadar benzer yapılarda olamamaktadır. Bu nedenle söz konusu birimlerde görev yapan personel rol ve sorumluluklarını Bilgi İşlem personeli kadar iyi ayırt edemeyebilirler.

BGYS kapsamına Bilgi İşlem birimi haricindeki birimlerin de dâhil edilmesi sonucu, bu birimlerin genel kabul görmüş organizasyon yapısına sahip olan Bilgi İşlem birimlerine göre daha spesifik organize edilmeleri nedeniyle, BGYS süreçlerinin bu birimlerde gerçekleştirilmesi işleri zorlaştırabilmektedir. Kapsam bu şekilde geniş tutulduğu durumlarda kapsama dâhil edilen her bir birimin iş süreçlerinde bilgi güvenliğinin sağlanmasına yönelik çalışmaların ayrı

ayrı özenle çalışılması gerekmektedir. İş süreçlerinin her bir kuruluşta ve her bir birimde farklı olması süreçlerde kullanılan bilgilerin güvenliklerinin sağlanmasını zorlaştırabilmektedir. BGYS kapsamının sadece Bilgi İşlem birimi olacak şekilde dar tutulmasında ise Bilgi İşlem birimlerinde standart yapıların var olması nedeniyle iş süreçlerinin benzer olması sayesinde bilgi güvenliğinin sağlanmasına yönelik çalışmalar da benzerlik taşımaktadır. Böylelikle kapsamın dar tutulduğu çalışmalar daha kolay bir şekilde gerçekleştirilebilmektedir.

BGYS kapsamının dar veya geniş tutulmasının etki ettiği bir diğer konuda maliyettir. Kapsamın sadece Bilgi İşlem birimi ile sınırlı kaldığı durumda BGYS süreçlerinin oluşturulması sadece bu birimde gerçekleştirileceği için ayrılacak kaynak miktarı daha az olacaktır. Ancak kapsamın tüm kuruluşu içerecek şekilde belirlenmesi durumunda, BGYS süreçleri tüm kapsam dâhilindeki birimlerde gerçekleştirileceğinden ayrılacak kaynak miktarı da belirlenen kapsamla doğru orantılı olarak artacaktır.

14.4. SONUÇ VE DEĞERLENDİRMELER

Kuruluşlar, bilgi güvenliğinin sağlanması amacıyla birçok çalışma yapmakta ve kaynak ayırmaktadırlar. Dünya çapında bir bilgi güvenliği standardı olarak kabul edilen ISO/IEC 27001 Standardı, kuruluşların bilgi güvenliği hedeflerini bir düzen eşliğinde gerçekleştirmeleri için bir altyapı sunmaktadır.

Standartta belirtilen BGYS kurulum ve işletim aşamaları düzenli bir şekilde yerine getirildiği takdirde, kuruluşlar bilgi güvenliği açısından önemli bir adım atmış olacaklardır. Kuruluşların sahip oldukları bilgi varlıklarının farkına varmasını sağlayarak bilgi varlıklarını koruma noktasında farkındalık oluşturmaktadır. Böylece, kuruluşun karşılaşabileceği maddi ve manevi kayıpların önüne geçilebilecektir. Bugün tüm kuruluşlarda veri genellikle dijital ortamlarda tutulmaktadır. Kuruluşlarda dijital ortamların sorumluluğu genellikle Bilgi İşlem birimlerine verilmektedir. Bu bağlamda Kuruluşlar BGYS kapsamlarının Bilgi İşlem birimi olarak belirlendiği durumlarda bilgi güvenliği ihtiyacını karşıladığını değerlendirebilmektedir. Oysa ki bilgi güvenliği; teknoloji, süreç ve insan faktörlerinin beraber değerlendirilmesi gereken ve bu üç faktöre göre oluşturulması gereken bir kavramdır [15].

Bilgi varlıkları dijital ortamlarda tutulsa da kuruluşların yapısı gereği Bilgi İşlem birimleri haricindeki birimlerde de ciddi güvenlik önlemi alınmasını

gerektiren bilgi varlıkları bulunabilmektedir. Bu tür kuruluşlarda BGYS kapsamının diğer birimleri de kapsayacak şekilde belirlenmesi önem arz etmektedir. Ancak kuruluşların yürüteceği ve yöneteceği BGYS çalışmaları kendi personeli ile hiçbir danışmanlık almadan gerçekleştirilecek ise ve kuruluşta bu çalışmaları yürütecek sayı ve nitelikte personel yok ise bu süreci yürütmek ve yönetmek ciddi sıkıntılar oluşturacaktır. Bu anlamda kuruluşun yapısı iyi analiz edilmeden, BGYS kapsamı belirlenmemelidir.

BGYS kapsamının Bilgi İşlem birimi haricindeki birimleri de kapsayacak şekilde tutulması hâlinde bilgi güvenliğinin sağlanmasına yönelik bütünlük sağlanabilecek ancak kapsamın bu şekilde geniş tutulması maliyeti ve iş gücünü arttıracak ve buna ek olarak bazı zorlukları da beraberinde getirecektir. Yapılan bir çalışma [10] BGYS'nin kurulacağı kapsam oluşturulurken mümkün olduğunca BGYS kapsamının kısıtlı tutulmasının uygulama açısından verimli olacağını, kapsam içerisinde varlık ve bu varlıklara ait risk analizlerinin teker teker yapılmasından dolayı kapsamın geniş tutulmasının dosya yığınlarına neden olacağını ve bunun gerçek anlamda sistemin oluşturulup yönetilmesinin önüne geçeceğini ifade etmektedir.

BGYS kapsamının dar ve geniş tutulduğu durumlarda meydana gelecek zorlukların karşılaştırması Tablo 14.1'de verilmiştir.

Tablo 14.1. BGYS Kapsamının Dar ve Geniş Tutulmasındaki Uygulama Zorluklarının Karşılaştırılması

Kolaylıklar	Zorluklar
BGYS Kapsamının Bilgi İşlem Birimi ile Sınırlı Tutulması (Dar Kapsam)	BGYS Kapsamına Bilgi İşlem Birimi Haricindeki Birimlerin Dahil Edilmesi (Geniş Kapsam)
Bilgi İşlem personelinin bilgi güvenliği konusunda bilgi ve farkındalık düzeyinin yüksek olması sebebiyle BGYS süreçlerinin oluşturulması ve işletilmesi daha kolaydır.	Bilgi İşlem harici birim personelinin bilgi güvenliği konusunda bilgi ve farkındalık düzeyinin Bilgi İşlem personeline göre daha düşük olması sebebiyle BGYS süreçlerinin oluşturulması ve işletilmesi daha zordur.
BGYS organizasyon yapısında Bilgi İşlem birimi personeli olacağından BGYS'nin süreçlerinin yönetilmesi daha kolaydır.	BGYS organizasyon yapısında Bilgi İşlem harici birimlerden personel de bulunacağından BGYS'nin yönetilmesi zordur.
BGYS organizasyon yapısında ve süreçlerin işletilmesinde Bilgi İşlem birimi yönetici ve personeli rol alacağından bürokrasi düşüktür.	BGYS organizasyon yapısında ve süreçlerin işletilmesinde Bilgi İşlem birimi haricindeki birimlerin yönetici ve personeli rol alacağından bürokrasi yüksektir.

Tek birim olduğundan birimde BGYS süreçlerinin entegrasyonu kolaydır.	Birden fazla birim olduğundan birimler arasında BGYS süreçlerinin entegrasyonu zordur.
Bilgi varlıkları envanteri daha dar kapsamlı ve yönetilebilirdir.	Bilgi varlıkları envanteri her birim özelinde olacağından ve birimler arası personel sirkülasyonunun çok olduğu kuruluşlarda çok daha geniş kapsamlı ve yönetilmesi zordur.
Bilgi varlıklarına ilişkin risklerin yer aldığı risk envanterinin yönetilmesi ve güncelliğinin sağlanması daha kolaydır.	Risk envanteri her birim özelinde bilgi varlıklarına ilişkin olacağından yönetilmesi ve güncelliğinin sağlanması zordur.
İç tetkik bir ekip ile gerçekleştirilebileceğinden iç tetkik sürecinin gerçekleştirilmesi kolaydır.	İç tetkikler birden fazla ekip vasıtasıyla gerçekleştirilebileceğinden ekiplerin bütünsel bir yaklaşım sergilemesinin zor olması sebebiyle iç tetkik sürecinin gerçekleştirilmesi zordur.
İç tetkik faaliyeti genel bilgi sistemleri bilgi seviyesi daha yüksek olan Bilgi İşlem birimi personeli ile gerçekleştirileceğinden iç tetkik faaliyetinin amacına uygun bir şekilde gerçekleştirilmesi kolaydır.	İç tetkik faaliyeti genel bilgi sistemleri bilgi seviyesi daha düşük olan diğer birim personeli ile gerçekleştirileceğinden iç tetkik faaliyetinin amacına uygun gerçekleştirilmesi zordur.
Tespit edilen uygunsuzluklara ilişkin düzeltici iyileştirici faaliyetlerin takibi, kapatılması ve imza/onay süreçlerinin yürütülmesi çok daha kolaydır.	Tespit edilen uygunsuzluklara ilişkin düzeltici iyileştirici faaliyetlerin takibi, kapatılması ve imza/onay süreçlerinin yürütülmesi zordur.
BGYS organizasyon yapısında Bilgi İşlem birimi personeli ve yöneticileri yer alacağından yönetim gözden geçirme toplantılarının organize edilmesi, mevcut durumun şeffaf bir şekilde tartışılması kolaydır.	BGYS organizasyon yapısında Bilgi İşlem harici birimlerde görev alan personel ve yöneticiler yer alacağından Yönetim gözden geçirme toplantılarının organize edilmesi, mevcut durumun şeffaf bir şekilde tartışılması zordur.
Bilgi güvenliği farkındalık eğitimleri kapsama alınan tüm personele kuruluş personeli tarafından verileceğinden sadece Bilgi İşlem birimi personelinin eğitim kapsamına dahil edilmesi, sürecin organize edilmesi, kısa bir zamanda gerçekleştirilmesi ve etkinliğinin ölçülmesi açısından daha kolaydır.	Bilgi güvenliği farkındalık eğitimleri kapsama alınan tüm personele kuruluş personeli tarafından verileceğinden kuruluşun tüm birim personelinin eğitim kapsamına dahil edilmesi, sürecin organize edilmesi ve etkinliğinin ölçülmesi açısından daha zordur ve uzun bir zaman alır.
Bilgi İşlem birimi organizasyon yapısı için genel kabul görmüş örnek yapıların var olması sebebiyle bilgi güvenliğinin sağlanmasına yönelik çalışmaların gerçekleştirilmesi kolaydır.	Bilgi İşlem harici birimlere ait genellikle genel kabul görmüş bir organizasyon yapısının var olmaması sebebiyle bilgi güvenliğinin sağlanmasına yönelik çalışmaların gerçekleştirilmesi zordur.
BGYS süreçlerinin sadece Bilgi İşlem biriminde gerçekleştirilmesinin maliyeti düşüktür.	BGYS süreçlerinin birden fazla birimde gerçekleştirilmesinin maliyeti yüksektir.

Tablo 14.1 değerlendirildiğinde BGYS'nin kurulmasında ve işletilmesinde karşılaşılan en büyük zorlukların genellikle insan kaynaklı olduğu görünmektedir. Kişilerin bilgi güvenliği konusundaki bilgi ve farkındalık düzeyleri birbirinden farklı olduğu için bilgi güvenliğine ilişkin bazı konular kişilerin bilgi düzeylerine göre tartışmalara neden olabilmektedir. BGYS kapsamının yönetilebilir boyutta tutulması önemlidir [11]. BGYS kapsamının Bilgi İşlem birimiyle sınırlı tutulduğu durumlarda, süreçlerin işletilmesi Bilgi İşlem personeli eliyle gerçekleştirileceği için BGYS'nin kurulması ve işletilmesi daha kolay olacaktır. Ancak insan kaynağı bilgi güvenliğinin en önemli halkası olduğu için bilgi güvenliği sadece kurumların Bilgi İşlem personeli ile değil tüm personelin ortak sorumlulukları ile yürütülebilecek bir süreçtir. Personel sayısı ve birimleşmenin nispeten daha fazla olduğu, birimler arası personel sirkülasyonunun fazla olduğu, iyi organize edilmiş bir bilgi teknolojileri alt yapısının ve yönetiminin olmadığı kurumlarda BGYS'nin kurulumu ve işletimi sürecinde bahsedilen zorluklarla yüzleşilmesi neredeyse kaçınılmazdır.

Aynı şekilde insan kaynaklı problemler BGYS süreçleri gerçekleştirilirken bürokrasinin artmasına da neden olabilmektedir. Yapılan bir çalışmada [12], BGYS'nin üst yönetim tarafından benimsendiği, kurumsal süreçlerin yönetilmesi ve kazandırdığı itibar açısından olumlu değerlendirildiği sonucuna ulaşılmıştır. Ancak BGYS tarafından getirilen bazı ek kontroller ve kısıtlamalar açısından üst yönetim tarafında ayrıcalık tanınması gerektiği yönünde görüşler olduğu da ifade edilmiştir. BGYS'nin etkin bir şekilde işletilmesi ve iyileştirilmesi süreçlerinde özellikle de yönetim kademesinde yer alan kişilerin tutum ve destekleri çok önemlidir. Kurum yönetimi tarafından kurulan BGYS'nin sahiplenilmesi gerekmektedir. Aksi takdirde kurumsal bilgi güvenliği yönetimlerinin etkinliği her zaman sorgulanmalıdır.

Kurum içerisinde BGYS çalışmasını sürdürecek bir organizasyonun oluşturulması gerekmektedir. BGYS kapsamına bilgi güvenliği konusundaki bilgi ve farkındalık düzeyleri yüksek, rol ve sorumlulukları spesifik olarak belirlenmiş olan personelin olduğu sadece Bilgi İşlem biriminin alındığı durumlarda BGYS organizasyon yapısı da genellikle bu birimde görev yapan yönetici ve personelden oluşmaktadır. Ancak diğer durumda bilgi güvenliği konusundaki bilgi ve farkındalık düzeyleri nispeten daha düşük, rol ve sorumlulukları net bir şekilde tanımlanmamış olan personelin olduğu diğer birimlerin kapsama alındığı durumda BGYS organizasyonu bu birimlerin yönetici ve personelinden oluşturulacaktır. Bunun sonucunda BGYS'nin oluşturulması ve işletilmesi süreçlerinde bürokratik engeller, bireysel sıkıntılar gibi zorluklarla

karşılaşılacak, farklı alan ve mesleklerden kişilerin bilgi güvenliği konusunda bir paydada buluşabilmesi zorluk oluşturacaktır.

Kapsam boyutlandırmanın sonucu olarak karşımıza çıkan diğer önemli husus ise maliyettir. İş süreçlerinin BGYS ile entegrasyonu, değişen varlıklar ve varlıklara ilişkin güncellenen riskler, risklerin ortadan kaldırılması için gerekli önlemler maliyetin belirlenmesi konusunda değişkenlerdir. Bu sebeple, BGYS süreçleri için ayrılacak kaynak miktarı belirlenen kapsam ile doğru orantılı olarak artacaktır.

BGYS süreçlerini işletirken en çok zaman alan konulardan birisi kuşkusuz iç tetkik faaliyetleridir. BGYS'nin gereği olan ve risklerin tespiti noktasında önem arz eden iç tetkik çalışmaları belirli bir plan dâhilinde yürütülen ve zaman alan bir çalışmadır. İç tetkik faaliyeti kapsamına ne kadar fazla birim, bilgi varlığı ve personel dâhil olursa süreç bir o kadar zorlaşmaktadır. İç tetkik faaliyetleri sonucunda yazılan raporların değerlendirilmesi, her birim yöneticisi tarafından incelenmesi ve imzalanması süreçlerinin uzun zaman alabilmesi; BGYS'nin devamlılığı sağlanması gereken ve belirli dönemlerde dış denetime tabi olan bir süreç olmasından kaynaklı olarak kuruluş personelini de sıkıntıya sokmaktadır.

Kuruluşlar; BGYS kapsamında yürütecekleri çalışmaları hiçbir danışmanlık hizmeti almadan kendi personeli ile gerçekleştirecekler ise, uygulanabilir ve etkin bir BGYS için kapsam analizi çalışmalarını titizlikle yapmalı, BGYS organizasyon yapısında yer alan personelin bu alandaki niteliğini değerlendirmeli, süreçlerde yer alacak personelin iş yükünü göz önünde bulundurmalı ve kuruluşun yapısını iyi analiz etmelidir. Aksi takdirde BGYS kapsamında yürütülen tüm çalışmaların etkin olduğundan bahsetmek zorlaşabilmektedir.

KAYNAKLAR

[1]. Ersoy, E. V. (2012). ISO/IEC 27001 Bilgi Güvenliği. Ankara: ODTÜ Yayıncılık.

[2]. Canbek, G. ve Sağıroğlu, Ş. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme. Politeknik Dergisi, 9, (3) 165-174.

[3]. Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. Scientific Research, 4 (2) 92-100.

[4]. (2013). TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı. Ankara: Türk Standardları Enstitüsü.

[5]. Susanto, H., Almunawar, M. ve Tuan, Y. (2012). A Novel Method on ISO 27001 Reviews: ISMS Compliance Readiness Level Measurement. Computer Science Journal, 2, (1) 1-12.

[6]. Özbilgin, İ. ve Özlü, M. (2010). Yazılım Geliştirme Süreçleri ve ISO 27001 Bilgi Güvenliği Yönetim Sistemi. 20. Akademik Bilişim 2018 Konferansı Bildirileri.

[7]. Angraini, Megawati ve Haris, L. (2018). Risk Assessment on Information Asset an academic Application Using ISO 27001. The 6th International Conference on Cyber and IT Service Management (CITSM 2018). Pekanbaru.

[8]. Almeida, R., Lourinho, R., Silva, M. ve Pereira, R. (2018). A Model for Assessing COBIT 5 and ISO 27001 Simultaneously. 2018 IEEE 20th Conference on Business Informatics (s. 60 - 69). Lisbon: IEEE Computer Society.

[9]. Marttin, V. ve Pehlivan, İ. (2010). ISO 27001:2005 Bilgi Güvenliği Yönetimi Standardı ve Türkiye'deki Bazı Kamu Kuruluşu Uygulamaları Üzerine Bir İnceleme. *Mühendislik Bilimleri ve Tasarım Dergisi* , 49-56.

[10]. Gencer, K. (2015). ISO 27001 Kapsamında Kurumsal Bilgi Güvenliğine Dinamik Bir Yaklaşım. Yayınlanmamış Yüksek lisans Tezi. Afyon: T.C. Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü.

[11]. Bingöl, U. (2010). ISO 27001 Bilgi Güvenliği Yönetim Sistemi Otomasyonu. *ISO 27001 Bilgi Güvenliği Yönetim Sistemi Otomasyonu*. Sakarya: T.C. Sakarya Üniversitesi Sosyal Bilimler Enstitüsü.

[12]. Tuygun, M. (2019). ISO27001 Bilgi Güvenliği Yönetim Sistemi Standardının Kamu Kurumlarına Uygulanabilirliğinin Araştırılması: Ankara İli Örneği. Ankara: Yayınlanmamış Yüksek Lisans Tezi. Gazi Üniversitesi Bilişim Enstitüsü.

[13]. Vural, Y. ve Sağıroğlu, Ş. (2008). Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme. Gazi Üniv. Müh. Mim. Fak. Der., 507-522.

[14]. Yılmaz, H. (2014-15). TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması Ve Bilgi Güvenliği Risk Analizi. Denetişim, 45-59.

[15]. Çek, E. (2017). Kurumsal Bilgi Güvenliği Yönetişimi Ve Bilgi Güvenliği İçin İnsan Faktörünün Önemi. İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı.

[16]. Turan, M. (2020). Medium: https://medium.com/@musttrn/bilgi-guvenligi-temel-kavramlari-771aed625870 adresinden alındı

[17]. Gülmüş, M. (2010). Kurumsal bilgi güvenliği yönetim sistemleri ve güvenliği. Yayınlanmamış YüksekLisans Tezi. T.C. Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Elektrik Mühendisliği AnaBilim Dalı.

[18]. Özdemir, A. (2019). Kamu Kurum ve Kuruluşlarında Bilgi Güvenliği Farkındalığı. Gazi Üniversitesi Bilişim Enstitüsü Adli Bilişim Ana Bilim Dalı.

[19]. Altınpulluk, Ö. (2016). Iso 27001:2013 Bilgi Güvenliği Yönetim Sistemi Kurumsal Risk Yönetimi. Iso 27001:2013 Bilgi Güvenliği Yönetim Sistemi Kurumsal Risk Yönetimi. İstanbul: T.C. Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü.

[20]. Haklı, T. (2012). Bilgi Güvenliği Standartları Ve Kamu Kurumları Bilgi Güvenliği İçin Bir Model Önerisi. Yayınlanmamış Yüksek Lisans Tezi. Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü. Isparta.

[21]. İren, E. ve Can, Ö. (2017). Bilgi Sistemlerinde Güncel Güvenlik Problemleri ve Önerilen Çözümler. TUBAV Bilim Dergisi, 10 (2) 27-42

Bölüm 15

SİBER TEHDİT İSTİHBARATI VE SALDIRI TESPİT SİSTEMLERİNDE BÜYÜK VERİ TEKNOLOJİLERİ

Yavuz Canbay

Dijitalleşen dünya ile beraber hayatımıza giren siber saldırılar önceleri basit ve tespit edilmesi kolay yapılar iken, günümüzde artık karmaşık bir yapı alarak tespit edilmesi zor hâle gelmiştir. Bu problemi çözme amacıyla, saldırıların gerçekleşmeden önce onlara ait istihbarat bilgilerinin toplanması, gerçekleştikten sonra ise tespit edilmesi günümüzün vazgeçilmez iki ana unsuru olmuştur. Özellikle son zamanlarda büyük veri teknolojilerinin de siber güvenlik alanına başarı ile uygulanması, gerek siber tehdit istihbaratı gerekse de saldırı tespit sistemlerinde bu teknolojilerden faydalanmayı zorunlu kılmıştır. Bu çalışmada, siber tehdit istihbaratı, saldırı tespit sistemleri ve büyük veri teknolojileri açıklanmış, büyük veri teknolojilerinden faydalanan siber tehdit istihbaratı ve saldırı tespit sistemlerine yönelik çalışmalar gözden geçirilmiş ve çeşitli değerlendirmelerde bulunulmuştur.

15.1. GİRİŞ

Siber saldırılar, bilgisayar sistemlerini hedef alarak bu sistemlerdeki zafiyetleri kullanıp, insanlara, kurum ve kuruluşlara zarar vermeyi amaçlayan aktivitelerdir. Geçmişte insanların eğlence, merak veya küçük hedefler doğrultusunda gerçekleştirdiği bu saldırılar, günümüzde doğrudan sistemleri hedef alan, planlı, organize, karmaşık ve gün geçtikçe daha da çok evrimleşen/değişen bir saldırı türü hâline gelmiştir [1].

Böylesi büyüyen, gelişen ve karmaşık hâle gelen saldırıların gerçekleşmeden önce gerekli önlemlerin alınabilmesi amacıyla tehdide yönelik istihbarat bilgilerinin toplanması ve analiz edilerek anlamlandırılması ve gerçekleşmesi hâlinde ise tespit edilmesi önemli rol oynar. Siber tehdit istihbaratı, "mevcut veya ortaya çıkan bir tehdit veya tehlike hakkında kapsam, mekanizmalar, göstergeler, çıkarımlar ve eyleme geçirilebilir tavsiyeler dâhil olmak üzere kanıta dayalı bilgi" olarak Gartner tarafından tanımlanmıştır [2].

Günümüz siber savunma sistemlerinin büyük çoğunluğu, siber saldırıları algılayan/tanıyan ve bunlara karşı önlemler alan sistemler olarak geliştirilmiştir. Örneğin bir saldırı önleme sistemi, saldırıları tespit etmek ve bunları engellemek üzerine geliştirilmiştir. Böylesi sistemler genel olarak statik ve dinamik yapılara sahip olsa da, özellikle bu sistemleri yöneten kişinin bilgisi kadar bir kabiliyete sahip olan sistemlerdir [3].

Siber saldırıların tespiti ve önlenmesi önemli olduğu kadar, böylesi eylemlerin gerçekleştirilmeden belirlenerek gerekli önlemlerin alınması da önemlidir. Özellikle herhangi bir saldırı gerçekleşmeden gerekli istihbarat bilgilerinin edinilmesi, o saldırının vereceği zararı daha gerçekleşmeden bertaraf etmeyi sağlamada kilit rol oynar.

Geçmişte basit virüslerle gerçekleştirilen siber saldırılar günümüze çok sayıda ve farklı türde tehditleri barındıran ve gittikçe karmaşıklaşan bir hâle gelmiştir. Örneğin APT saldırısı kendi bünyesinde oltalama, kötücül yazılım, arka kapı, DNS yönlendirme gibi farklı türde tehditleri içeren tek bir saldırı türüdür. Saldırıların bu şekilde farklılaşmasının ana sebebi, klasik yani bilinen saldırı türlerinin savunma sistemleri tarafından kolayca tespit edilebilmesidir. Bu yüzden saldırılar gittikçe karmaşık hâle gelmekte, başka bir ifadeyle evrimleşmektedir. Böylesi bir durum, doğal olarak saldırıların tespitini de zorlaştırmaktadır [4].

Her geçen gün sistemlerde meydana gelen zafiyetlerin artmasıyla beraber bu zafiyetleri kullanan saldırı çeşitleri ve sayıları artmakta olup, siber güvenlik uzmanlarının bu saldırılar karşısında sürekli kendilerini güncel tutmaları, ortaya çıkan bu saldırıları analiz etmeleri ve bunlardan haberdar olmaları uzun süre alabilmektedir [5]. Yeni çıkan bir saldırının uzun süre sonrasında siber güvenlik uzmanları tarafından belirlenip ona karşı bir savunma mekanizma-

sının geliştirilmesi sürecine kadar geçen zaman zarfında kurum bu saldırıya maruz kalmış, kurumdan kritik bilgiler sızdırılmış, kurum tamamen tehdit altında kalmış olabilmektedir [6].

Dolayısıyla ortaya çıkan yeni tehditlerin istihbarat bilgileri çerçevesinde tespit edilmesi, bu saldırıların siber güvenlik uzmanlarına haber verilmesi ve gerekli savunma mekanizmaların geliştirilmesi sürecinin kısaltılması konusunda büyük önem taşır.

[5] numaralı çalışmada yapılan araştırmada bildirildiği üzere, gerçekleştirilen bir saldırının uzmanlar tarafından tespit edilmesi EMEA ülkeleri için ortalama 469 gün iken dünya genelinde ortalama 169 gün olduğu belirtilmiştir. Özellikle APT gibi gelişmiş tekniklerin kullanıldığı bu saldırılarda, yukarıda belirtilen sürenin uzun olmasından dolayı aslında saldırganın kurum içindeki pek çok bilgiyi de dışarı sızdırabileceği önemli bir gerçektir.

Siber tehdit istihbaratı her ne kadar önemli bir konu olsa da özellikle gerek pek çok farklı ortamdaki verilerin toplanması ve gerekse de onların analiz edilmesi klasik analitik süreçleri ile zordur. Siber tehdit istihbaratında bilgi kaynağı olarak sıklıkla tercih edilen internet dünyası, hem yapısal hem de yapısal olmayan pek çok verileri barındırmaktadır. Böylesi platformlarda tutulan verilerin hacim, hız ve çeşitliliklerinin yüksek olmasından dolayı büyük veri teknolojilerinden faydalanmak en önemli araç olacaktır.

İnternet üzerinde forumlar, bloglar, sosyal mecralar, raporlar, araştırmalar gibi çeşitli platformlarda yazılan metinler önemli varlıklardır. Keşfedilen yeni bir zafiyeti kullanarak gerçekleştirilecek yeni bir saldırının ortaya çıkması durumunda, bu saldırı ile ilgili çeşitli bilgiler bu platformlarda kullanıcıların bilgisine sunulabilmektedir. Dolayısıyla sürekli gelişen ve büyüyen dinamik bir yapı olan bu platformların incelenerek yeni zafiyetlerin tespitinin sağlanması güvenlik uzmanlarına önemli bir avantaj sağlayacaktır. Özellikle DarkNet gibi internetin karanlık yüzü olan bu platformlarda korsan gruplarının fikir alışverişinde bulunduğu forumlar ve bloglar öncelikle üzerinde durulması gereken platformlardır [7].

Siber tehdit istihbaratının genel amacı her ne kadar muhtemel tehditleri bir sistem vasıtasıyla hızlı bir şekilde tespit ederek siber güvenlik uzmanlarının bu tehditlerden haberdar olmasını olabildiğince erken süreye çek-

mek olsa da bu yeni tehditlerin analiz edilerek bir sonraki saldırının hangi özellikleri barındırabileceğinin tahmin edilmesini sağlamak da önemli bir unsurdur. Bu amaçla, tahminleyici (predictive) sistemler geliştirilmek gereklidir [8].

Genel olarak bir siber tehdit istihbarat sistemi, SurfaceWeb ve DarkWeb üzerindeki korsan (hacker) forumları ve blogları ile diğer çeşitli sosyal medya platformlarındaki yapısal olmayan veri türü olan metinler üzerinde çalışır. Böylesi bir sistem eğitim aşamasında durağan veriler üzerinde işlem yaparken, tespit aşamasında akan veriler üzerinde işlem yapar ve genel olarak sürekli aktif olarak tarama ve tespit işlemini sağlar. Ayrıca, MISP, CybOX, STIX ve TAXII gibi platformlar da siber istihbarat verilerini paylaşan çeşitli platformlardır.

Ülkemizde meydana gelen siber olaylar ve tehditler dikkate alındığında, yeni tehditleri tespit ederek uyarı oluşturan mekanizmalara her zaman için ihtiyaç vardır. 2016-2019 Ulusal Siber Güvenlik Stratejisi Eylem Planında [9] belirtilen "Tehdit unsurlarının saldırı yapmadan önce bertaraf edilmesi için ulusal proaktif siber savunma yeteneğinin geliştirilmesi" maddesine katkı sağlamak önemli olup bu kapsamda ülkemizde geliştirilen çeşitli yazılımlar da mevcuttur.

15.2. SİBER TEHDİT İSTİHBARATI

Günümüzde özellikle gelişen teknoloji ile beraber siber saldırganların hareket kabiliyetleri artmış, ortaya çıkan yeni teknolojilerde bulunabilecek muhtemel zafiyetleri tespit ve onları kullanma kapasiteleri de üst seviyeye çıkmıştır. Yeni zafiyetlerin ortaya çıkması, siber saldırganların dikkatini çekmekte ve pek çok zaman bu zafiyetleri kullanarak yeni tehditler oluşturabilmektedirler.

Siber alanda muhtemel gelebilecek tehditlere karşı istihbarat bilgileri toplamak önemli bir proaktif yaklaşımdır. Bir saldırının gerçekleşmeden bertaraf etmek, saldırının muhtemel vereceği zararları da bertaraf etmek demektir. Bundan dolayı özellikle siber istihbarat bilgilerini toplamak önemlidir.

Gelişen teknolojinin bir çıktısı olarak ortaya konulan yeni sistemlerde veya hâlihazırda bulunan mevcut sistemlerde tespit edilen bir zafiyetin kurumun siber güvenlik birimleri tarafından tespiti ve takibi uzun zaman alabilmektedir. Klasik yaklaşımlarda, siber tehditlerin kurum siber güvenlik birimleri tarafından toplanması ve anlamlandırılması yapılırken, tehdit havuzunun büyümesiyle beraber aslında bu işlem bir yerden sonra otomatik olarak yapılması gereken bir işlem hâlini almıştır.

Siber tehdit istihbaratı yapısı ile karmaşık bir problem olup, pek çok farklı kaynaktan alınan verilerin birleştirilmesi ve analiz edilerek anlamlandırılması ile sağlanır. Böyle karmaşık bir problem için literatürde sunulan çözümlere ek olarak aslında bu verileri genel amaç için toplayıp paylaşan çeşitli platformlar da mevcuttur. [10] numaralı çalışmada önerilen TAXII'de bunlardan biridir.

Şekil 15.1'de gösterildiği üzere, siber tehdit istihbarat türlerini stratejik, taktik, operasyonel ve teknik olarak 4 farklı kategoride ele almak mümkün olup bunlar aşağıda açıklanmıştır [11].

Şekil 15.1. Siber istihbarat türleri [11]

Stratejik tehdit istihbaratı; karar vericiler tarafından kullanılan yüksek seviyede bilgilerdir. Teknik bilgileri içermekten ziyade, siber saldırının finansal boyutu saldırı eğilimlerini ve iş kararlarına etkileri gibi bilgileri içeren rapor formatında bilgilerdir.

Operasyonel tehdit istihbaratı; kuruma karşı yaklaşan saldırıları içeren ve yüksek seviyede güvenlik personeli tarafından kullanılan bilgilerdir.

Taktik tehdit istihbaratı; tehdit aktörlerinin saldırıları nasıl yürüttükleri hakkında bilgidir. Taktiksel tehdit istihbaratı, siber olaylara müdahale ekiplerinin savunma becerilerini, uyarı ve analizlerinin mevcut taktiklere hazır olması için kullanılır.

Teknik tehdit istihbaratı; teknik anlamda kullanılan verilerdir. Saldırganlar tarafından kolayca değiştirilebileceği için kullanım süresi kısa olan bilgilerdir.

Yukarıda belirtilen dört farklı istihbarat türü de önemli yapılar olup, özellikle teknik anlamda toplanan istihbarat bilgilerinin mevcut tehdidi önleme adına önemi büyüktür.

Şekil 15.2'de gösterildiği üzere, siber tehdit istihbaratı genel olarak 6 aşamadan oluşur. Bunlar;

- **Planlama:** tehditlere yönelik gerekli istihbarat bilgilerinin belirlenmesi,
- **Toplama:** belirlenen kaynaklardan verilerin toplanması,
- **İşleme:** toplanan ham verinin analize hazır hâle getirilmesi,
- **Analiz etme:** analize hazır hâle getirilen verinin işlenerek gerekli istihbarat bilgilerinin elde edilmesi,
- **Dağıtma:** ilgili birimlere istihbarat bilgilerinin paylaşılması,
- **Geri bildirim:** elde edilen istihbarat verilerinin ihtiyaçları karşılayıp karşılamadığına yönelik geri bildirimler alma.

Şekil 15.2. Siber tehdit istihbaratı yaşam döngüsü [12]

Yeni güvenlik zafiyetlerini belirlemek için değişen siber tehdit istihbaratı için büyük veri teknolojileri kaçınılmazdır. Öncelikli olarak uzun zamanlı bir analiz gerçekleştirebilmek için geçmiş verilerinin tutulması gerekir. Böylesi verileri de doğru bir şekilde analiz edebilmek için büyük veri teknolojilerine ihtiyaç vardır. Epostalar, sosyal medya içerikleri, kurum dokümanları ve web içerikleri gibi yapıların büyük çoğunluğu yapısal olmayan veri formatındadır. Analiz edilecek verilerin büyük hacimli olması, onların gerçek zamanlı analizinde büyük bir sorun teşkil etmesine karşılık büyük veri teknolojileri ile bu sorun kolaylıkla çözülebilmektedir [13].

15.3. SALDIRI TESPİT SİSTEMLERİ

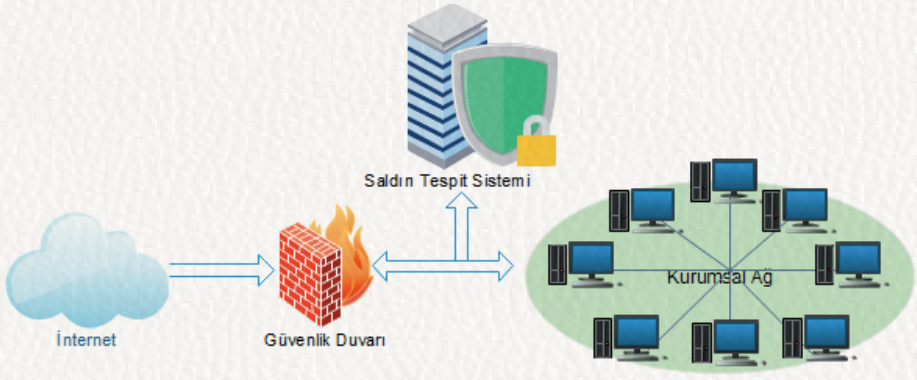
Saldırganların çeşitli yöntemler kullanarak bilgisayar sistemlerine yetkisiz ve izinsiz bir şekilde sızma girişimlerinin hepsine saldırı denilmektedir. Saldırıların tespiti, belirlenmesi ve raporlanması için kullanılan kaynaklar, metotlar

ve araçların tümüne saldırı tespit sistemleri denilmektedir [14]. Saldırı tespit sistemlerinin genel amaçları, geleneksel güvenlik duvarları ile tespit edilemeyen farklı türdeki kötücül network trafiği ve bilgisayar kullanımlarını belirlemektir. Saldırı tespit sistemleri genel olarak iki farklı kategoride değerlendirilir. Bunlar imza tabanlı ve anomali tabanlıdır [15].

İmza tabanlı saldırı tespit sistemlerinde, daha önce bilinen bir saldırının örüntüsünü eşleştirerek yeni saldırıları belirleme işlemi yapılır. Burada örüntü eşleştirmeden kasıt imza ya da başka bir ifadeyle özet karşılaştırmadır. Başka bir ifadeyle, potansiyel saldırıların imzaları çıkarılarak daha önce bilinen saldırıların imzası ile karşılaştırılması sonrası eşleştirme olması hâlinde bir alarm üretilir ve bu şekilde saldırı tespiti sağlanır. Bu yaklaşım, bilinen saldırılara karşı etkili olsa da 0. gün gibi bilinmeyen saldırılara karşı başarısızdır [16].

Anomali tabanlı saldırı tespit sistemlerinde ise sistemin normal davranışı, makine öğrenmesi, istatistiksel ve bilgi tabanlı metotlarla oluşturulur. Gözlemlenen davranışlar eğer belirlenen bu normal davranışlara aykırı düşerse bu durumda bir anomalinin oluştuğu ve mevcut davranışın saldırı olduğu belirlenir. Bu sistemlerde özellikle 0. gün gibi daha önce bilinmeyen saldırıların tespiti mümkündür [17].

Genel bir saldırı tespit sistemi mekanizması Şekil 15.3'te gösterilmiştir. Saldırı tespit sistemleri şekilden de görüleceği üzere kurum ağı içerisindeki hareketleri izleyerek saldırı veya kötüye kullanımları tespit edip raporlamayı sağlar.



Şekil 15.3. Genel bir saldırı tespit sistemi mekanizması

APT saldırıları özellikle karmaşık yapısından dolayı tespiti zor bir saldırı tekniğidir. APT saldırıları sıklıkla ya kullanıcıların giriş bilgilerini ya da 0. gün zafiyetlerini kullanarak sistemde bir alarm oluşturmadan sisteme erişim sağlar. Genel olarak sistemlerdeki hassas nitelikli bilgileri çalmayı hedefleyen bu saldırılar karmaşık ve farklı türde saldırıları içerisinde barındırmaktadır. Genellikle sahte epostalar ile kullanıcıyı kandırarak kötücül yazılım indirip çalıştırmasını ister. Böylesi bir saldırıyı tespit etmede büyük veri teknolojilerinden faydalanmak en akıllıcasıdır. Gerek analiz edilecek verinin miktarının fazla olması gerekse de bu verilerin faklı tipte ve farklı kaynaklardan geliyor olması büyük veri teknolojilerini kullanmayı zorunlu kılar [18].

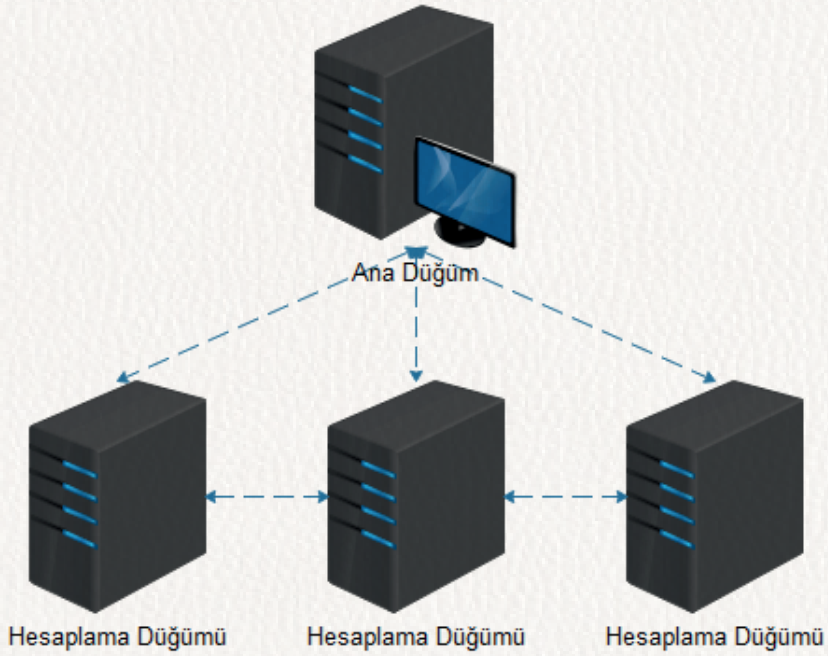
15.4. BÜYÜK VERİ VE TEKNOLOJİLERİ

Büyük veri kavramı, Gartner'ın raporunda "daha iyi sezgi, karar verme ve süreç otomasyonunu mümkün kılan maliyet etkin, yenilikçi bilgi işleme biçimleri talep eden yüksek hacimli, yüksek hızlı ve/veya çok çeşitli bilgi varlıkları" [19] olarak tanımlanmıştır. Büyük veri, günümüzde pek çok alanda sıklıkla kullanılan önemli bir teknoloji hâline gelmiştir. Büyük devletler başta olmak üzere sıklıkla kullanılan büyük veri teknolojileri günümüzün önemli araçlarından biri hâline gelmiştir. Ekonomiden sağlığa, ülke yönetiminden iletişime kadar pek çok alanda faydalanılan büyük veri kavramı; özellikle politika belirleme, strateji geliştirme, gelecek planlama, kurum bazlı tahmin ve analiz yapma gibi çeşitli alanlarda büyük imkânlar sunan önemli bir yapıdır. Özellikle kabul edilebilir bir sürede analiz edilemeyen çeşitli türlerde verilerin yönetimi, analizi, depolanması, anlamlandırılması ve görselleştirilmesi gibi konularda karşılaşılan zorlukların aşılması amacıyla ortaya çıkan bir kavramdır [20-22]. İlk olarak hacim, hız ve çeşitlilik bileşenlerine sahip olarak ortaya çıkan büyük veri kavramı, zamanla değişen veya evrimleşen problemlerin çözümü için değer, doğruluk ve değişkenlik gibi pek çok bileşene de sahip olmuştur [22-28]. Bu bileşenlerden bazıları aşağıda kısaca açıklanmıştır;

- **Hacim:** Verinin depolama biriminde kapladığı alanı temsil eder.
- **Hız:** Verinin belirli periyotlardaki üretim frekansına karşılık gelir.
- **Çeşitlilik:** Veri kaynaklarında üretilen verinin formu olarak tanımlanır. Yapısal, yapısal olmayan ve yarı-yapısal olmak üzere üç kategoride sınıflandırılır.

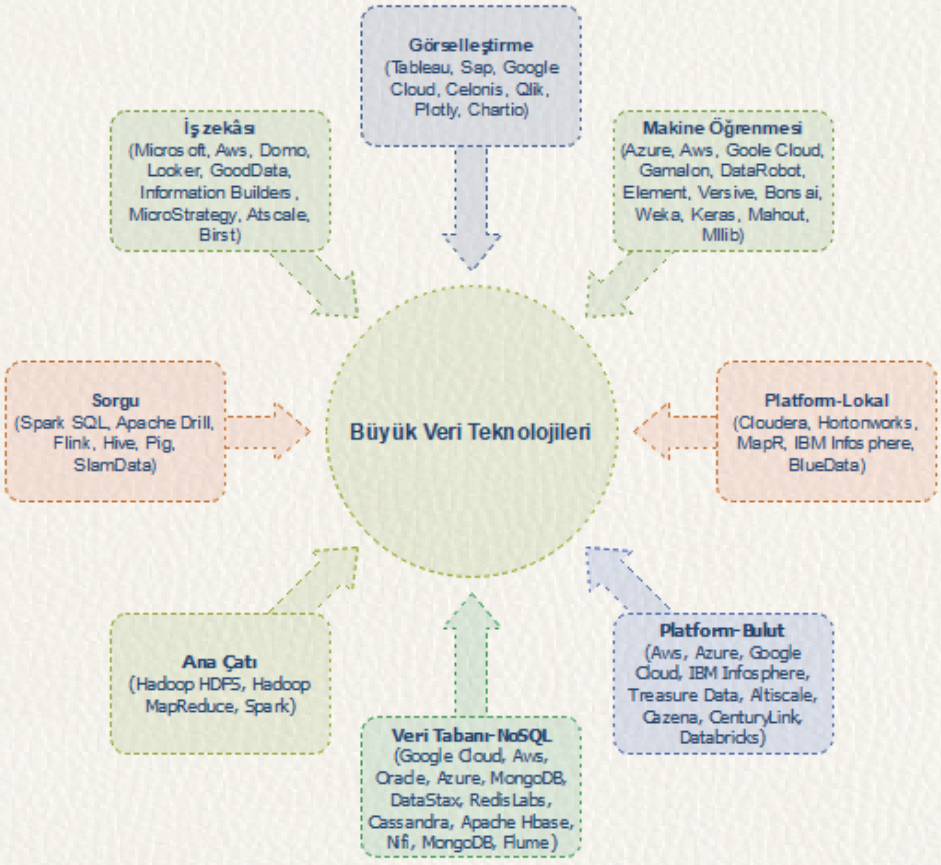
- **Değer:** Büyük veriden elde edilecek faydayı temsil eder.
- **Doğruluk:** Verinin doğruluğunu ve güvenilirliğini belirtir.
- **Değişkenlik:** Verinin içerisinde bulunabilecek muhtemel tutarsızlıkları (aykırı veri, eksik veri vb.) ifade eder.

Dağıtık bir yapıdan oluşan büyük veri mimarisi, temel işleri yerine getiren bir ana düğüme ve hesaplama işlerinden sorumlu birden fazla hesaplama düğüme sahiptir. Efendi ve köle mimarisine dayalı olarak çalışan bu mimaride, ana düğüm büyük veri kümesini küçük parçalara ayırıp veri düğümlerine iletirken, hesaplama düğümleri ise kendi üzerindeki veri parçalarında paralel olarak ilgili işleri yapar. Bu mimaride yer alan sistemler, tüm düğümlerde aynı yazılım, donanım ve ağ teknolojisi yapısına sahip olan homojen yapılardır. Bu sistemlerde yüksek hızlı ağ üzerinden veri transferi yapılırken, standart ağ üzerinden ilgili haberleşmeler sağlanır [29]. Şekil 15.4'te dağıtık mimari için bir örnek verilmiştir.



Şekil 15.4. Büyük veride dağıtık mimari yapısı

Büyük veri mimarisi üzerinde bir analitik işlemi yapmak için çeşitli teknolojilere ihtiyaç duyulur. Bu ihtiyaçlar kapsamında hangi teknolojilerin kullanılacağına doğru karar vermek gerekir. Aksi hâlde, analitik süreci doğru bir şekilde yürütülemez ve beklenen çıktılar elde edilemez. Büyük veri teknolojileri, hizmet ettiği alana özgü çeşitli sınıflara ayrılmaktadır. Şekil 15.5'te büyük veri analitiğinde kullanılan çeşitli teknolojiler ve bunların kullanıldığı çeşitli alanlar gösterilmektedir.



Şekil 15.5. Alanlara göre büyük veri teknolojileri [30, 31]

15.5. SALDIRI TESPİT SİSTEMLERİ VE SİBER TEHDİT İSTİHBARATINA YÖNELİK YAPILAN ÇALIŞMALAR

Literatürde, büyük veri teknolojilerini kullanarak geliştirilen saldırı tespit sistemleri ve siber tehdit istihbaratı çözümleri aşağıda özetlenmiştir.

15.5.1. Büyük Veri Teknolojileri Kullanılarak Geliştirilen Saldırı Tespit Sistemleri

Büyük veri teknolojilerini kullanarak saldırı tespit sistemi geliştiren güncel bazı çalışmalar aşağıda özetlenmiştir.

- Ratrohe ve arkadaşları [14], toplama, filtreleme, yük dengeleme ve işleme katmanlarına sahip büyük veri mimarisi temelli bir saldırı tespit sistemi önerdiler. DARPA veri kümesinin kullanıldığı çalışmada, Hadoop, Spark ve Mapreduce teknolojilerinden faydalanılmıştır.
- Ahn ve arkadaşları tarafından yapılan çalışmada [32], bilinmeyen türdeki saldırıların tespiti için büyük veri analizi sistemine sahip bir konsept oluşturulmuştur. Bilinmeyen APT saldırılarını tespit etmek ve önlemek için büyük veri analizi üzerine dayalı bir model geliştirilmiştir. Veriler güvenlik duvarı, kayıt veya günlük (log) dosyaları, kullanıcı davranışı, antivirüs veri tabanından çeşitli bilgiler, ağ cihazları ve sistemleri gibi yapılardan toplanarak elde edilmiştir. NoSQL, Hadoop ve MapReduce gibi teknolojiler kullanılarak istenilen gereksinimle karşılanıp ön işlem aşaması tamamlanmıştır. Veriler, tahmin, sınıflandırma, birliktelik analizi, kullanıcı davranışı, sistem durumu gibi yapılar analiz edilmiştir. Bu analiz sonucunda eğer bir saldırı veya anormal davranış tespit edildiğinde sistem yöneticiye uyarı vermektedir.
- Shenwen ve arkadaşlarının yaptığı çalışmada [33], büyük veri mimarisi kullanılarak APT saldırısının tespitine yönelik bir çözüm sunulmuştur. Bu sistem ile hem bilinen hem de bilinmeyen APT saldırıları tespit edilebilmektedir. Sistem, veri toplama, büyük veri işleme, APT analizi ve uygulama katmanı olarak 4 aşamadan oluşmaktadır. Hadoop ve Mahout teknolojileri kullanılarak, ağ verisi, sistem kayıtları ve çeşitli güvenlik bilgileri analiz edilmiştir.

- Goutam ve arkadaşlarının yaptığı çalışmada [34], büyük veri mimarisi üzerinde gerçek zamanlı saldırı tespit sistemi geliştirilmiştir. Bu sistem, yakalama katmanı, filtreleme ve yük dengeleme katmanı, işleme katmanı, karar verme katmanı olmak üzere 4 katmandan oluşmaktadır. Büyük veri teknolojilerinden olan Apache Storm kullanılarak gerçek zamanlı bir hibrit saldırı tespit sistemi geliştirilmiştir. 85 GB büyüklüğünde, ISCX firması tarafından oluşturulan saldırı tespit sistemi verileri kullanılmıştır. CC4 sinir ağı yapısı ile bilinmeyen saldırılar tespit edilirken, Çok katkı yapay sinir ağı (MLP-Multi-layered Perceptron) ile de kötüye kullanım tespiti sağlanmış ve %89 başarı elde edilmiştir.
- Machal ve arkadaşlarının yaptığı çalışmada [35], büyük ölçekteki güvenlik verilerinin gözlemlenmesi için bir büyük veri mimarisi geliştirilmiştir. DNS verisi, NetFlow kayıtları, http trafiği ve balküpü verileri analiz edilmiştir. Büyük veri teknolojilerinden olan Hadoop ve Spark kullanılmıştır.
- Othman ve arkadaşları [36], KDDCUP99 veri seti üzerinde Apache Spark çerçevesi ile destek vektör makineleri ve lojistik regresyon yöntemlerini kullanarak saldırı tespit sistemi geliştirmişlerdir. Öznitelik seçimi için ChiSquare yönteminin kullanıldığı çalışmada, klasik yöntemlerle yapılan karşılaştırma sonrası elde edilen deney sonucuna göre önerilen yöntemin daha başarılı olduğu gözlemlenmiştir.
- Vieira ve arkadaşları [37], büyük veri mimarisi üzerinde saldırı tespiti yapan bir sistem geliştirdiler. Kendi ürettikleri network verileri üzerinde MapReduce ve Hadoop yapılarından faydalandılar. Geliştirdikleri imza tabanlı saldırı tespit sistemi ile yüksek tespit başarısı elde ettiler.
- [38] numaralı çalışmada, Microsoft Azure platformu kullanılarak saldırı tespit sistemi geliştirip bu sistemi KDDCUP99 veri kümesi ile test edilmiştir. Karar ağacı ve sinir ağları algoritmalarının kullanıldığı çalışmada, Chisquare ve Mutual Information yöntemlerinden faydalanılarak öznitelik seçme işlemi gerçekleştirdiler. Yapılan testler sonucunda yüksek başarı elde ettiler.
- Ratrohe ve arkadaşları [39], Hadoop ve Spark teknolojilerinden faydalanarak bir saldırı tespit sistemi geliştirdiler. Bu sistemi KDDCUP99

veri kümesini kullanarak test ettiler. Önerdikleri sistemde altı farklı sınıflandırma algoritması kullandılar.

- [40] numaralı çalışmada, Microsoft Azure platformu üzerinde k2 adını verdikleri bir sınıflandırma algoritması kullanarak bir saldırı tespit sistemi geliştirmişlerdir. MAWILab veri kümesinin kullanıldığı çalışmada, Spark teknolojisinden faydalandılar.
- Zhang ve arkadaşları [41], Spark teknolojisi üzerinde Random Forest algoritmasını kullanarak büyük veri mimarisine uygun bir saldırı tespit sistemi geliştirmişlerdir. CICIDS2017 veri kümesi üzerinde test edilen sistemin, farklı algoritmalara göre daha yüksek başarı sağladığı belirtilmiştir.

Yukarıda sunulan çalışmalar, Tablo 15.1'de dört farklı parametreye göre karşılaştırılmıştır. Bu tabloya göre saldırı tespit sistemlerinde, en çok kullanılan büyük veri teknolojilerinin Spark ve Hadoop oldukları, en çok kullanılan veri kümesinin KDDCUP99 olduğu ve genel olarak sınıflandırma tabanlı olarak çalışmaların tercih edildiği görülmektedir.

Tablo 15.1. Literatürdeki çalışmaların karşılaştırılması

Çalışma	Veri Kümesi	Kullanılan Teknoloji	Amaç	Odak
[14]	DARPA, KDDCUP99	Spark, Mapreduce, Hadoop	Saldırı tespit sistemi	Sınıflandırma
[32]	Farklı kaynaklardan toplanan veriler	No-Sql, Hadoop, MapReduce	Saldırı tespit sistemi	APT tespiti
[33]	Farklı kaynaklardan toplanan veriler	Hadoop, Mahout	Saldırı tespit sistemi	APT tespiti
[34]	ISCX verisi	Apache Storm	Saldırı tespit sistemi	Sınıflandırma
[35]	Network trafik verisi	Hadoop, Hive, Pig, Spark, Shark	Saldırı tespit sistemi	Korelasyon
[36]	KDDCUP99	Spark	Saldırı tespit sistemi	Sınıflandırma
[37]	Farklı kaynaklardan toplanan veriler	Hadoop, MapReduce	Saldırı tespit sistemi	İmza
[38]	KDDCUP99	Azure	Saldırı tespit sistemi	Sınıflandırma
[39]	KDDCUP99	Hadoop, Spark	Saldırı tespit sistemi	Sınıflandırma
[40]	MAWILab	Azure, Spark	Saldırı tespit sistemi	Sınıflandırma
[41]	CICIDS2017	Spark	Saldırı tespit sistemi	Sınıflandırma

15.5.2. Büyük Veri Teknolojileri Kullanılarak Geliştirilen Siber Tehdit İstihbarat Sistemleri

Literatürde büyük veri teknolojileri kullanılarak geliştirilen siber tehdit istihbarat sistemlerine ait çalışmalar aşağıda özetlenmiştir.

- Tao ve arkadaşları [42], bilgi sistemlerinden topladıkları statik ve dinamik veriler ile üçünü parti bileşenlerden topladıkları istihbarat bilgilerini birleştirip büyük veri ortamında analiz etmiştir. Geliştirdikleri ortamda, çevrimdışı (offline) hesaplamada statik veri analizi için Hadoop, Hive, HBase ve Mapreduce teknolojilerinden; ara (nearline) hesaplamada HBase, HDFS ve Spark teknolojilerinden; çevrimiçi (online) hesaplamada dinamik veri analizi için ise Storm teknolojisinden faydalanılmıştır.
- Chen ve arkadaşlarının yaptıkları çalışmada [6], açıklıların daha ortaya çıkmadan tahmin edilmesi ve düzeltilmesi için büyük veri yaklaşımı önerilmiştir. Proaktif siber güvenlik sistemi olarak sunulan bu yapıda, açıklık veri tabanları, saldırı veri tabanları ve bunlara ek olarak korsanların tartışmalarının, paylaşımlarının yer aldığı forumlar, bloglar, IRC platformları taranmıştır. Metinler üzerinden çalışılmıştır. Potansiyel atakların belirlenmesi ve önleyici karşı önlemler geliştirilmesi amaçlanmıştır. Sistem temel olarak konunun belirlenmesi ve bu konunun takibi üzerine kurulmuştur. Konu kümeleme işlemi ile yeni çıkan konuyu tespit edilmesi ve yeni konu grupları ile ilgili yeni korsan topluluklarının tespit edilmesi sağlanacağı belirtilmektedir.
- Charles ve arkadaşları [43] siber tehdit istihbaratı için büyük veri mimarisi önerdiler. Apache Kafka kullanılarak gerçek zamanlı veri toplama işleme yapılarak, 100 GB'lık gerçek network verisinden tehdit istihbaratına yönelik çıkarımlarda bulundular. Dört farklı algoritma ile yapılan sınıflandırma işleminde başarılı sonuçlar elde edilmiştir.

Yukarıdaki çalışmalar incelendiğinde, özellikle siber tehdit istihbaratında büyük veri teknolojilerinden faydalanan çalışmaların az sayıda olduğu görülmektedir. Bu durumun gerekçeleri şu şekilde sıralanabilir;

- İlk ve en önemli husus bu tür verilerin hassas veriler olması sebebiyle paylaşılmak istenilmemesidir.
- Siber tehdit istihbaratı için istihbarat paylaşımı yapan platformların sundukları bilgiler yeterli görülüp buna ek bir büyük veri mimarisi temelli sistem geliştirilmek istenmeyebilir,

- Korsan forumlarından, sosyal mecralardan, DarkWeb gibi platformlardan elde edilen ham html verilerinin büyük veri mimarilerinde analiz edilmesinin zor olması,
- DarkWeb ve Korsan forumları gibi platformlardan veri toplamanın zor olması olarak belirtilebilir.

15.5.3. Siber Tehdit İstihbarat Sistemleri Üzerine Yapılan Çalışmalar

Siber tehdit istihbaratına yönelik bazı güncel çalışmalar aşağıda özetlenmiştir.

- Macdonald ve arkadaşları [44], korsan forumlarından topladıkları veriler üzerinde doğal dil işleme yaklaşımları ile tehditlere ilişkin anahtar kelime çıkarma ve korsanların kritik alt yapılar için kullandıkları ifadeleri belirleme işlemi yapılmıştır. Open Discussion Forum Crawler programı aracılığıyla veriler toplanmış ve alana özgü olarak bir duygu analiz işlemi gerçekleştirilmiştir. Siber korsanlar tarafından oluşturulan her bir post için duygu analizi yapılmış ve skorlanmıştır.
- Kadoguchi ve arkadaşları çalışmalarında [7], DarkWeb'de bulunan forum sitelerinde siber istihbarat toplamak için bir yaklaşım geliştirmiştir. Doğal dil işleme ve makine öğrenmesi tekniklerinin kullanıldığı çalışmada, Sixgill isimli bir siber istihbarat platformunu kullanarak DarkWeb'den korsan aktivitelerine ilişkin çeşitli bilgiler topladılar. Doc2vec yapısını kullanarak metinleri vektör hâline getirip daha sonra MLP ağı ile sınıflandırma işlemi yaptılar.
- Hamad ve arkadaşları yaptıkları çalışmada [45] balküpünden (honeypot) elde ettikleri verileri analiz ederek değerlendirdikleri yeni bir tehdit istihbarat tekniği önerdiler. Elasticsearch yaklaşımını kullanarak 500MB büyüklüğünde bir kayıt veya günlük (kayıt) dosyası analiz ettiler. Pek çok farklı sınıfta saldırı olayları istatistiksel olarak analiz edilmiştir.
- Landauer ve arkadaşları yaptıkları çalışmada [46], kayıt dosyası analiz ederek siber tehdit istihbaratı için çeşitli bilgiler elde etmeye çalışmıştır. Anomali tespiti yaklaşımı kullanılarak gerçekleştirilen uygulamada, tespit edilen anomalilerin tehdit istihbaratına dönüştürülmesi aşaması açıklanmıştır.

- Gao ve arkadaşları [47] siber tehdit istihbaratının modellenmesi ve tehdit tiplerinin belirlenmesi için bir sistem geliştirdiler. IBM X-Force Exchange ve VirusTotal platformlarından toplanan tehdit istihbarat verileri üzerinde analiz yapmışlardır.
- Yürekten ve Demirci'nin yaptıkları çalışmada [48], farklı kaynaklardan toplanan istihbarat verilerini değerlendiren, kurumların kendi bünyelerinde yazılım tabanlı ağlar için otomatik ağ yapılandırması yapan bir model geliştirmişlerdir. Geliştirilen model altı farklı veri kümesi kaynağında test edilmiş ve yazılım tanımlı ağlar için kurallar üretilmiştir.

Yukarıda özetlenen çalışmalar dikkate alındığında, siber tehdit istihbaratı için veri kaynağı olarak DarkWeb, forum siteleri, kayıt dosyaları, balküpü verileri ve özellikle çeşitli açık kaynak platformlardan faydalanıldığı görülmektedir.

15.6. SONUÇ VE DEĞERLENDİRMELER

Kurumsal bilgi güvenliğini sağlamada siber tehdit istihbaratı ve saldırı tespit sistemleri günümüzün vazgeçilmez iki ana unsurudur. Saldırıların gerçekleşmeden önce onlara dair bilgilerin toplanarak ilgili önlemlerin hızlıca alınması gerekir. Bu aşamada, özellikle siber güvenlik uzmanlarının bilgi ve becerileri önemli olsa da, hızla gelişen ve değişen teknolojiler ve bunların barındırdığı zafiyetleri takip etmek kolay olmayıp aynı zamanda bunların takibi uzun zaman almaktadır. Bundan dolayı gerek siber güvenlik uzmanlarının istihbarat bilgilerini edinimini kolaylaştırmak gerekse de bu bilgileri toplamada geçen süreyi azaltmak amacıyla siber tehditlere yönelik istihbarat toplayan sistemlere büyük ihtiyaç vardır.

İstihbarat bilgilerinin toplanacağı alanlarda elde edilen bilgilerin çeşitliliği ve boyutu yüksek miktarda olduğundan dolayı bu tür verilerin büyük veri formuna gireceği için büyük veri teknolojileri kullanılarak bir sistem geliştirmek en doğru çözümdür.

Ağ üzerinde akan verinin miktarı gün geçtikçe arttığı için saldırı tespit sistemlerinde büyük veri mimarisine dayalı çözüm geliştirmek en doğrusudur. Özellikle analiz tarafında kullanıcılara ölçeklenebilirlik, paralel ve dağıtık hesaplama, hata toleransı gibi avantajlar sunan büyük veri teknolojilerinden mevcut probleme özgü olarak uygun teknolojilerin kullanılması, etkin bir saldırı tespit sistemi geliştirmede büyük kolaylık sağlayacaktır.

Literatürde yukarıda belirtilen iki alanda yapılan çalışmalar incelendiğinde;

- Özellikle büyük veri teknolojilerinden faydalanılan saldırı tespit sistemi çalışmalarının çok sayıda olduğu ve bundan dolayı da belirli bir olgunluğa eriştiği gözlemlenmiştir.
- Siber tehdit istihbaratında büyük veri teknolojileri açısından bakıldığında, yayımlanmış az sayıda çalışmaya rastlanmıştır. Bu durumun muhtemel gerekçeleri önceki bölümde belirtilmiştir.

Bu çalışma kapsamında yapılabilecek değerlendirmeler aşağıda sunulmuştur;

- Büyük veri teknolojileri pek çok alanda olduğu gibi siber güvenlik alnında da büyük avantajlar sağladığı için bu alanda büyük veri mimarisi temelli çözümlerin sayısının arttırılması gerektiği,
- Saldırı tespit sistemlerinde sıklıkla kullanılan büyük veri teknolojilerinden özellikle kurumsal yapılar için siber tehdit istihbaratı toplama ve analiz etmede de faydalanmak gerektiği,
- Çeşitli platformlardan paylaşılan siber tehdit istihbarat bilgileri ile yetinilmeyip bu alanda gerek kurumsal gerekse de ülke çapında siber tehdit istihbaratı toplama çözümlerinin sayısının arttırılması gerektiği,
- Siber tehdit istihbarat verilerin analiz edilmesi aşamasında büyük veri teknolojilerinin büyük önemi olduğu ve bu teknolojilerden faydalanılması gerektiği,
- Saldırı tespit sistemlerinde özellikle ağın sürekli dinlenmesi ile elde edilen akan verinin analizinin önemli olduğu ve bundan dolayı Spark Streaming gibi büyük veri teknolojilerinden faydalanılması gerektiği,
- Siber tehdit istihbaratında DarkWeb'in yapısına uygun tarama ve bilgi toplama çözümlerinin büyük veri mimarisi ile uyumlu olacak şekilde geliştirilmesi ve sayısının arttırılması gerektiği,
- Siber tehdit istihbarat verilerinin toplanıp analiz edilmesiyle elde edilen bilgilerin hızlı bir şekilde uygulamaya geçirilmesi ve tespit edilen zafiyetlerin hızlıca giderilmesi gerektiği,
- Siber güvenlik uzmanlarının tehdit istihbaratının elde edilebileceği mecraları doğru bir şekilde belirlemesi ve bu bilgilerini sürekli olarak güncel tutmaları gerektiği,

- Büyük veri teknolojileri kullanılarak geliştirilen saldırı tespit sistemlerinde imza tabanlı çalışması hâlinde mevcut imzaların sürekli güncel tutulması gerektiği,
- Büyük veri teknolojileri kullanılarak geliştirilen saldırı tespit sistemlerinde anomali tabanlı çalışması hâlinde ise yanlış-pozitif (false positive) oranını mümkün olduğu kadar minimize edilmesi gerektiği

değerlendirilmektedir.

Teşekkür

Bu çalışmaya verdiği desteklerden dolayı, Kahramanmaraş Sütçü İmam Üniversitesi Data Vision Laboratuvarına (https://datavision.ksu.edu.tr) teşekkür ederim.

KAYNAKLAR

[1] U. Ben-Porat, A. Bremler-Barr ve H. Levy, "Vulnerability of network mechanisms to sophisticated DDoS attacks," *IEEE Transactions on Computers,* vol. 62, pp. 1031-1043, 2013.

[2] Gartner. (06.06.2020). *Threat Intelligence*. Available: https://www.gartner.com/en/documents/2487216/definition-threat-intelligence

[3] M. Sato, H. Yamaki ve H. Takakura, "Unknown attacks detection using feature extraction from anomaly-based ids alerts," in *IEEE/IPSJ 12th International Symposium on,Applications and the Internet (SAINT),* 2012, pp. 273-277.

[4] R. Koch, M. Golling ve G. Dreo, "Attracting sophisticated attacks to secure systems: A new honeypot architecture," in *Communications and Network Security (CNS), 2013 IEEE Conference on*, 2013, pp. 409-410.

[5] B. Hau, M. Penrose, T. Hall ve M. Bevilacqua, "M-Trends 2016: EMEA Edition," 2016.

[6] H.-M. Chen, R. Kazman, I. Monarch ve P. Wang, "Predicting and fixing vulnerabilities before they occur: a big data approach," in *Proceedings of the 2nd International Workshop on BIG Data Software Engineering*, 2016, pp. 72-75.

[7] M. Kadoguchi, S. Hayashi, M. Hashimoto ve A. Otsuka, "Exploring the Dark Web for Cyber Threat Intelligence using Machine Leaning," in *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 2019, pp. 200-202.

[8] M. A. Rahman, Y. Al-Saggaf ve T. Zia, "A Data Mining Framework to Predict Cyber Attack for Cyber Security," in *2020 15th IEEE Conference on Industrial Electronics and Applications (ICIEA)*, 2020, pp. 207-212.

[9] *2016-2019 Ulusal Siber Güvenlik Stratejisi*. İnternet Sayfası: https://www.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf

[10] J. Connolly, M. Davidson ve C. Schmidt, "The trusted automated exchange of indicator information (taxii)," *The MITRE Corporation,* pp. 1-20, 2014.

[11] D. Chismon ve M. Ruks, "Threat intelligence: Collecting, analysing, evaluating," *MWR InfoSecurity Ltd,* 2015.

[12] (08.09.2020). *What is cybr threat intelligence?* İnternet Sayfası: https://hackersterminal.com/cyber-threat-intelligence-cti/

[13] V. Dheap. (23.08.2020). *What You Need to Know About Security Intelligence with Big Data*. İnternet Sayfası: https://securityintelligence.com/security-intelligence-with-big-data-what-you-need-to-know/

[14] M. M. Rathore, A. Ahmad ve A. Paul, "Real time intrusion detection system for ultra-high-speed big data environments," *The Journal of Supercomputing,* vol. 72, pp. 3489-3510, 2016.

[15] A. Khraisat, I. Gondal, P. Vamplew ve J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity,* vol. 2, p. 20, 2019.

[16] F. M. Cortés ve N. G. Gómez, "A hybrid alarm management strategy in signature-based intrusion detection systems," in *2019 IEEE Colombian Conference on Communications and Computing (COLCOM)*, 2019, pp. 1-6.

[17] A. Aldweesh, A. Derhab ve A. Z. Emam, "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues," *Knowledge-Based Systems,* vol. 189, p. 105124, 2020.

[18] C. S. Alliance. (12.06.2020). *Big Data Analytics for Security Intelligence*. İnternet Sayfası: https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Big_Data_Analytics_for_Security_Intelligence.pdf

[19] M. A. Beyer ve D. Laney, "The Importance of Big Data: A Definition," Gartner2012.

[20] K. Nandini Prasaad and T. Pratheek, "Providing Anonymity Using Top Down Specialization on Big Data Using Hadoop Framework," in *IEEE Annual India Conference*, New Delhi, India, 2015, pp. 1-6.

[21] H. K. Patil ve R. Seshadri, "Big Data Security and Privacy Issues in Healthcare," in *IEEE International Congress on Big Data* Anchorage, AK, USA, 2014, pp. 762-765.

[22] N. Victor, D. Lopez ve J. H. Abawajy, "Privacy Models for Big Data: A Survey," *International Journal of Big Data Intelligence,* vol. 3, pp. 61-75, 2016.

[23] X. Zhang, C. Yang, S. Nepal, C. Liu, W. Dou ve J. Chen, "A Mapreduce Based Approach of Scalable Multidimensional Anonymization for Big Data Privacy Preservation on Cloud," in *International Conference on Cloud and Green Computing*, Karlsruhe, Germany, 2013, pp. 105-112.

[24] W. Li ve H. Li, "LRDM: Local Record-Driving Mechanism for Big Data Privacy Preservation in Social Networks," in *IEEE International Conference on Data Science in Cyberspace*, Changsha, China, 2016, pp. 556-560.

[25] I. Olaronke ve O. Oluwaseun, "Big Data in Healthcare: Prospects, Challenges and Resolutions," in *Future Technologies Conference*, San Francisco, USA, 2016, pp. 1152-1157.

[26] M. Tanwar, R. Duggal ve S. K. Khatri, "Unravelling Unstructured Data: A Wealth of Information in Big Data," in *International Conference on Reliability, Infocom Technologies and Optimization*, Noida, India, 2015, pp. 1-6.

[27] W. Vorhies. (2014). *How Many V's in Big Data? The Characteristics that Define Big Data*. İnternet Sayfası: https://www.datasciencecentral.com/profiles/blogs/how-many-v-s-in-big-data-the-characteristics-that-define-big-data

[28] (05.08.2020). *Big Data: Data Wrangling Boot Camp Big Data Vs*. İnternet Sayfası: http://www.cs.odu.edu/~ccartled/Teaching/2017-Spring/DataWrangling/Presentations/030-bigDataVs.pdf

[29] A. Tanenbaum ve M. Van Steen, *Distributed Systems: Principles and Paradigms*. USA: Prentice-Hall, 2007.

[30] D. O. Matt Turck. (05.05.2020). *Great Power, Great Responsibility: The 2018 Big Data & AI Landscape*. İnternet Sayfası: http://mattturck.com/bigdata2018/

[31] V. Ankam, *Big Data Analytics*. UK: Packt Publishing, 2016.

[32] S.-H. Ahn, N.-U. Kim ve T.-M. Chung, "Big data analysis system concept for detecting unknown attacks," in *16th International Conference on Advanced Communication Technology*, 2014, pp. 269-272.

[33] L. Shenwen, L. Yingbo ve D. Xiongjie, "Study and research of APT detection technology based on big data processing architecture," in *Electronics Information and Emergency Communication (ICEIEC), 2015 5th International Conference on*, 2015, pp. 313-316.

[34] G. Mylavarapu, J. Thomas ve A. K. TK, "Real-time hybrid intrusion detection system using apache storm," in *2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems*, 2015, pp. 1436-1441.

[35] S. Marchal, X. Jiang, R. State ve T. Engel, "A Big Data Architecture for Large Scale Security Monitoring," in *2014 IEEE International Congress on Big Data*, 2014, pp. 56-63.

[36] S. M. Othman, F. M. Ba-Alwi, N. T. Alsohybe ve A. Y. Al-Hashida, "Intrusion detection model using machine learning algorithm on Big Data environment," *Journal of Big Data,* vol. 5, p. 34, 2018.

[37] K. Vieira, F. L. Koch, J. B. M. Sobral, C. B. Westphall ve J. L. de Souza Leão, "Autonomic Intrusion Detection and Response Using Big Data," *IEEE Systems Journal,* 2019.

[38] N. Rachburee ve W. Punlumjeak, "Big data analytics: feature selection and machine learning for intrusion detection on microsoft azure platform," *Journal of Telecommunication, Electronic and Computer Engineering (JTEC),* vol. 9, pp. 107-111, 2017.

[39] M. M. Rathore, A. Paul, A. Ahmad, S. Rho, M. Imran ve M. Guizani, "Hadoop based real-time intrusion detection for high-speed networks," in *2016 IEEE global communications conference (GLOBECOM)*, 2016, pp. 1-6.

[40] A. Abid ve F. Jemili, "Intrusion Detection based on Graph oriented Big Data Analytics," *Procedia Computer Science,* vol. 176, pp. 572-581, 2020.

[41] H. Zhang, S. Dai, Y. Li ve W. Zhang, "Real-time distributed-random-forest-based network intrusion detection system using Apache spark," in *2018 IEEE 37th International Performance Computing and Communications Conference (IPCCC)*, 2018, pp. 1-7.

[42] Y. Tao, Y.-x. Zhang, S.-y. Ma, K. Fan, M.-y. Li, F.-m. Guo*, vd.*, "Combining the big data analysis and the threat intelligence technologies for the classified protection model," *Cluster Computing,* vol. 20, pp. 1035-1046, 2017.

[43] C. Wheelus, E. Bou-Harb ve X. Zhu, "Towards a big data architecture for facilitating cyber threat intelligence," in *2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 2016, pp. 1-5.

[44] M. Macdonald, R. Frank, J. Mei ve B. Monk, "Identifying digital threats in a hacker web forum," in *Proceedings of the 2015 IEEE/ACM international conference on advances in social networks analysis and mining 2015*, 2015, pp. 926-933.

[45] H. Almohannadi, I. Awan, J. Al Hamar, A. Cullen, J. P. Disso ve L. Armitage, "Cyber threat intelligence from honeypot data using elasticsearch," in *2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)*, 2018, pp. 900-906.

[46] M. Landauer, F. Skopik, M. Wurzenberger, W. Hotwagner ve A. Rauber, "A Framework for Cyber Threat Intelligence Extraction from Raw Log Data," in *2019 IEEE International Conference on Big Data (Big Data)*, 2019, pp. 3200-3209.

[47] Y. Gao, L. Xiaoyong, P. Hao, B. Fang ve P. Yu, "HinCTI: A Cyber Threat Intelligence Modeling and Identification System Based on Heterogeneous Information Network," *IEEE Transactions on Knowledge and Data Engineering,* 2020.

[48] Ö. Yürekten ve M. Demirci, "Using cyber threat intelligence in SDN security," in *2017 International Conference on Computer Science and Engineering (UBMK)*, 2017, pp. 377-382.

DİZİN

YAZARLAR

EDİTÖRLER

Prof. Dr. Şeref Sağıroğlu

Gazi Üniversitesi Mühendislik Fakültesi
Bilgisayar Mühendisliği Bölümü
Bilgi Güvenliği Derneği II. Başkanı

Prof. Sağıroğlu, ülkemizde bilgi güvenliği, siber güvenlik ve büyük veri analitiği, güvenliği ve mahremiyeti konularında çalışmalar yapmaktadır. 20'nin üzerinde yayınlanmış kitabı bulunmaktadır. Biri amerikan patenti olmak üzere alınmış ve müracaat aşamasında olan 10'un üzerinde patenti , 100'ün üzerinde ulusal ve uluslararası indeksli dergilerde yayınlanmış makalesi ile 300'e yakın ulusal ve uluslararası yayımlanmış bildirisi ve 6000'in üzerinde atıfı bulunmaktadır. Bilgi güvenliği alanında iki akademik derginin de editörlüğünü yapmaktadır.

Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (www.iscturkey.org), IEEE Uluslararası Bilgisayar Bilimleri ve Mühendisliği Konferansı (www. ubmk.org), IEEE Uluslararası Makine Öğrenmesi ve Uygulamaları Konferansı (www.icmla-conferences.org), Büyük Veri Analitiği, Güvenliği ve Mahremiyeti Ulusal Kamu Çalıştayı (bigdatacenter.gazi.edu.tr), Ulusal Siber Terör Konferansı (www.siberteror.org), Açık Veri Türkiye Konferansı (www.acikveriturkiye.org), Siber Güvenlik ve Savunma Çalıştayı (www.iscturkey.org) gibi konferansların başkanlığını veya eşbaşkanlığını yürütmüş/yürütmektedir.

Bilgi Güvenliği Derneği (BGD), Türk Bilim Araştırma Vakfı (TÜBAV), Geleceği Önemseyenler Derneği (GÖNDER) Kurucu Üyesidir. İlki dönem, BGD Yönetim Kurulu Başkanlığı ve TÜBAV Genel Başkanlığı Gazi Üniversitesi Fen Bilimleri Enstitüsü Müdürlüğü gibi görevleri yürütmüştür.

Gönüllü olarak pek çok sosyal projeyi de yürütmüş olan Sağıroğlu, TÜBİTAK, Avrupa Birliği, BAP gibi Bilimsel Araştırma Projelerde de görev almış ve projeler yürütmüştür. Ulusal ve uluslararası konferanslarda, Bilgi Güvenliği, Büyük Veri, Siber Güvenlik ve Savunma, Yapay Zeka, Biyometrik Uygulamalar, İnovasyon Kültürü Oluşturma gibi konularda davetli konuşmacı olarak seminer ve konferanslar vermiştir.

Gazi Üniversitesi Ve Erciyes Üniversitesi Bilgisayar Mühendisliği Bölüm Başkanlığı, ISACA Ankara Chapter Akademi Koordinatörlüğü gibi görevleri yürütmüştür. Yükseköğretim Kurulu Siber Güvenlik Çalışma Grubu Üyeliği, Bilim Sanayi ve Teknoloji Bakanlığı Yazılım Sektörü Çalışma Grubu Üyeliği, BGD Yönetim Kurulu Üyeliği, IPV6Forum Turkey Başkanlığı, IEEE üyeliği, ACM Üyeliği, Avrupa ETSI Standartları

Gözlemci Komisyon Üyeliği gibi görevleri yürütmektedir. Havelsan, Kişisel Verileri Koruma Kurumu, Bilgi Teknolojileri ve İletişim Kurumu, gibi kurumlarda danışmanlık yapmıştır. Şu anda ise Gazi Üniversitesi Mühendislik Fakültesi Dekanlığı görevini yürütmektedir.

Doç. Dr. Sedat Akleylek

Ondokuz Mayıs Üniversitesi, Bilgisayar Mühendisliği Bölümü Doçent Doktor, Samsun Hesaplamalı Bilimler Doktora Programı A.B.D. Başkanı

Doç. Dr. Sedat Akleylek, İzmir doğumludur. 2004 yılında Ege Üniversitesi Matematik Bölümü'nde lisans eğitimini tamamlamıştır. Öğretim Üyesi Yetiştirme Programı kapsamında sırasıyla 2008 ve 2010 yıllarında yüksek lisans ve doktora çalışmalarını ODTÜ Uygulamalı Matematik Enstitüsü Kriptografi Programı'nda tamamlamıştır. 2012 yılında Almanya Bochum Ruhr Üniversitesi Donanım Güvenliği Grubu'nda, Almanya'da ve 2014-2015 yıllarında Almanya Darmstadt Teknik Üniversitesi Kriptografi ve Bilgisayar Cebri Grubu'nda misafir öğretim üyesi olarak görev almıştır. 2016 yılında Bilgisayar/Bilişim Bilimleri ve Mühendisliği, Bilgi Güvenliği ve Kriptoloji alt alanında doçent ünvanını almıştır. 2011 yılından bu yana Ondokuz Mayıs Üniversitesi, Bilgisayar Mühendisliği Bölümü'nde akademik hayatına devam etmektedir. Doç. Dr. Sedat Akleylek, kuantum sonrası kriptografi, verimli kriptografik hesaplamalar, Boolean fonksiyonlar ve siber güvenlik için uygulamalı kriptografi alanlarında çalışmalarını sürdürmektedir. Ulusal ve uluslararası kapsamda bilgi güvenliği ve kriptoloji alanında TÜBİTAK, Malezya UTAR, KOSGEB, Üniversite-Sanayi İş Birliği Projeleri ve Üniversiteler tarafından desteklenen Bilimsel Araştırma Projelerinde yürütücü, araştırmacı ve danışman olarak görevler almıştır. Doç. Dr. Sedat Akleylek, SCI-Expanded kapsamındaki uluslararası saygın üç dergide bilgi güvenliği ve kriptoloji alan editörlüğü görevlerini sürdürmektedir.

YAZARLAR

Öğr. Gör. Aykut Karakaya

Bülent Ecevit Üniversitesi, Bilgisayar Teknolojileri Bölümü,
Öğretim Görevlisi, Zonguldak

Zonguldak'ın Kdz. Ereğli ilçesinde doğan Öğr. Gör. Aykut Karakaya, 2013 yılında Samsun Ondokuz Mayıs Üniversitesi Bilgisayar Mühendisliği Bölümü'nde lisans eğitimini tamamlamıştır. Aynı bölümde sırasıyla 2014-2017 yılları arasında araştırma görevlisi olarak çalışmış ve 2016 yılında yüksek lisans çalışmalarını tamamlamıştır. 2016 yılında aynı üniversitenin Hesaplamalı Bilimler Doktora Programı'nda doktora çalışmalarına başlamış ve hâlen devam etmektedir. 2017 yılında Zonguldak Bülent Ecevit Üniversitesi Devrek Meslek Yüksekokulu'nun, Bilgisayar Teknolojileri Bölümü İnternet ve Ağ Teknolojileri Programı'nda öğretim görevlisi olarak çalışmaya başlamıştır ve hâlen bu görevini sürdürmektedir. Öğr. Gör. Aykut Karakaya bilgisayar ağları, veri iletişimi, bilgi güvenliği, algılayıcı ağlar ve nesnelerin interneti alanlarında akademik çalışmalarını sürdürmektedir.

Doç. Dr. Hidayet Takcı

Sivas Cumhuriyet Üniversitesi
Bilgisayar Mühendisliği Bölümü

htakci@cumhuriyet.edu.tr

Dr. Hidayet Takcı, 1974 yılında Sivas/Gürün'de dünyaya geldi. İlk ve orta öğrenimini Gürün'de tamamladıktan sonra sırayla; 1997 yılında Trakya Üniversitesi Bilgisayar Mühendisliği lisans programını, 1999 yılında Gebze Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliği yüksek lisans programını, 2005 yılında Gebze Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliği doktora programını tamamlayarak Doktor Bilgisayar Yüksek Mühendisi unvanını aldı.

Bugüne kadar; Gebze Yüksek Teknoloji Enstitüsü, Kocaeli Üniversitesi, Okan Üniversitesi ve Ahmet Yesevi Üniversitesinde (Uzaktan Eğitim) dersler veren Dr. Takcı 2011 yılından bu yana Sivas Cumhuriyet Üniversitesi Bilgisayar Mühendisliği bölümünde öğretim üyesi olarak görev yapmaktadır. 2016 yılından bu yana Gürün Meslek Yüksekokulu Müdürlüğü, 2018 yılından bu yana Sivas Cumhuriyet Üniversitesi Meslek Yüksekokulları Koordinatörlüğü ve 31 Aralık 2019 tarihinden bu yana Sivas Cumhuriyet Üniversitesi Bilgisayar Mühendisliği bölüm başkanlığı görevlerini yürüten Dr. Takcı Bilgisayar Mühendisliği Bölümünde Bilgisayar Yazılımı Doçenti olarak akademik ve idari çalışmalarına devam etmektedir.

Hüseyin Akarslan

Emniyet Amiri
Terörle Mücadele Daire Başkanlığı

2006 yılında Polis Akademisi'nden mezun olan Emniyet Amiri Hüseyin AKARSLAN, Emniyet Genel Müdürlüğü'nün Bilgi Teknolojileri ve Siber Suçlarla ilgili birimlerinde farklı rütbe ve pozisyonlarda görev almıştır. 2011 yılında yüksek lisans eğitimini Güvenlik Bilimleri Enstitüsü, Adli Bilimler Ana Bilim Dalı'nda "Bilişim Suçları, Bilişim Yoluyla İşlenen Suçlar ve Adli Bilişim Ayrımı" başlıklı teziyle tamamlamıştır. Ulusal ve uluslararası birçok proje ve akademik etkinlikte yer alan yazar hâlen Terörle Mücadele Daire Başkanlığında Bilgi Teknolojileri Şube Müdürü olarak görev yapmakta ve doktora eğitimine Gazi Üniversitesi, Bilişim Enstitüsü, Yönetim Bilişim Sistemleri Ana Bilim Dalı'nda devam etmektedir.

Pelin Özkaya

Avukat, Ankara Barosu

Ankara doğumlu olan Pelin Özkaya, 2009 yılında İşletme Fakültesinden, 2015 yılında Hukuk Fakültesinden mezun olmuştur. Ankara Üniversitesi Adli Bilimler Enstitüsü Adli Bilişim bölümünde yüksek lisans öğrencisi olup, tez aşamasındadır. Ankara Barosuna kayıtlı olarak, kendi kurduğu hukuk ofisinde serbest avukatlık yapmaktadır. Adli Bilişim, Bilişim Hukuku, Kişisel Verilerin Yönetimi ve Fikri-Sınai Mülkiyet alanları başta olmak üzere, diğer hukuki konularda da danışmanlık, dava takibi yapmakta ve eğitim faaliyetlerini sürdürmektedir. Ankara Barosu Bilişim Teknoloji ve Hukuk Kurulu, Kişisel Verilerin Korunması Hukuku Kurulu ve Fikri Mülkiyet Rekabet Hukuku Kurulu üyesidir. Biyometri, Siber Güvenlik, Bilgi Güvenliği, Yapay Zekâ, Fikri ve Sınai Mülkiyet, Kişisel Veri ve Adli Bilişim konularında araştırmalarını sürdürmekte, uluslararası hukuki düzenlemeler ve mahkeme kararları ile teknik uygulamalar ve standartlarla ilgilenmektedir. Aynı zamanda bilimsel dergilere makaleler yazmaktadır.

Prof. Dr. Refik Samet

Ankara Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü Öğretim Üyesi, Ankara

Azerbaycan doğumlu olan Samet, ülkemizde bilgisayar sistemlerinin güvenilirliği, arıza-kaldırılabilirliği, bilgi güvenliği, siber güvenlik, kötü amaçlı yazılım analizi ve adli bilişim konularında çalışmalar yapmaktadır. 6 patenti, 1 kitabı ve 3 kitap bölümü bulunmaktadır. 50'ye yakın ulusal ve uluslararası indeksli dergilerde yayınlanmış makalesi ile 60'ın üzerinde ulusal ve uluslararası yayınlanmış bildirisi bulunmaktadır. 50'in üzerinde TÜBİTAK, NATO, Avrupa Birliği, BAP gibi Bilimsel Araştırma ve Üniversite Sanayi İş Birliği Projelerinde de görev almış ve projeler yürütmüştür. Birçok Ulusal ve Uluslararası Bilim Konferanslarında ve Dergilerinde Bilim Kurulu üyeliği yapmaktadır. Hâlen Ankara Üniversitesi Bilgisayar Mühendisliği Bölümünde Profesör olarak çalışmaktadır.

Hande Tutumluer

Lisans eğitimini Hacettepe Üniversitesi Fen Fakültesi İstatistik Bölümü'nde tamamlamıştır. Çeşitli projelerde veri analisti olarak görev almasının ardından kamuda bilgi teknolojileri alanında göreve başlamıştır. Siber Güvenlik, Adli Bilişim, Davranışsal Biyometriler, Adli Psikoloji ve Büyük Veri başlıca ilgi alanları olmakla beraber hâlen Ankara Üniversitesi Adli Bilimler Enstitüsü Adli Bilişim Bölümü'nde yüksek lisans eğitimine devam etmektedir. İngilizce ve Rusça bilmektedir.

Bilgehan Arslan

Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü Öğretim Görevlisi, Ankara.

2013 yılında Süleyman Demirel Üniversitesi Bilgisayar Mühendisliğinden mezun olan Bilgehan Arslan, yüksek lisans derecesini 2015 yılında Gazi Üniversitesinden almıştır. Gazi Üniversitesi Bilgisayar Mühendisliği bölümünde 2014 yılında Araştırma Görevlisi olarak işe başlamıştır ve hâlen aynı üniversitede Öğretim Görevlisi olarak çalışmaktadır. 2015 yılından beri Gazi Üniversitesinde doktora çalışmalarına devam etmektedir. Biyometri, Görüntü İşleme, Makine Öğrenmesi, Derin Öğrenme ve Bilgi Güvenliği gibi konular üzerinde akademik çalışmalarını sürdürmektedir.

Çağla Aksoy

Genelkurmay Başkanlığı Bilgisayar Mühendisi
cagla.aksoy1@gazi.edu.tr

2012 yılında Eskişehir Osmangazi Üniversitesi Bilgisayar Mühendisliği bölümünden mezun olan Çağla AKSOY, yüksek lisans derecesini 2017 yılında Gazi Üniversitesinden almıştır. 2017 yılından beri Gazi Üniversitesi Adli Bilişim bölümünde doktora çalışmalarına devam etmektedir.

Hami Satılmış

Ondokuz Mayıs Üniversitesi, Bilgisayar Mühendisliği Bölümü,
Araştırma Görevlisi, Samsun

Samsun ili Bafra ilçesi doğumlu olan Hami Satılmış, 2011 yılında başladığı Eskişehir Osmangazi Üniversitesi Bilgisayar Mühendisliği lisans eğitimini 2016 yılında bitirdi. 2017 yılında Ondokuz Mayıs Üniversitesi Bilgisayar Mühendisliği Bölümü'nde başladığı yüksek lisans eğitimini 2020 yılında tamamladı. 2020 yılında Ondokuz Mayıs Üniversitesi Hesaplamalı Bilimler Bölümü'nde başladığı doktora eğitimine devam etmektedir.

Kuantum sonrası kriptografi, bilgi güvenliği ve yazılım mühendisliği çalışma alanlarında akademik çalışmalarını sürdürmektedir.

Habibe Güler

Habibe Güler 1994 senesinde Sivas/Merkez'de dünyaya geldi. İlk ve orta öğrenimini burada tamamladı. 2019 yılında Gazi Üniversitesi Bilgisayar Mühendisliği Bölümü'nden mezun oldu. Aynı sene Gazi Üniversitesinde başlamış olduğu yüksek lisans eğitimini sürdürmektedir. 2020 yılının mart ayında Gazi Üniversitesi Bilgisayar Mühendisliği Bölümü'nde Araştırma Görevlisi olarak işe başlayan Habibe Güler hâlen bu görevine devam etmektedir. Bilgi Güvenliği, Siber Güvenlik ve Makine Öğrenmesi gibi konularda akademik çalışmalar yapmaktadır.

Dr. Öğr. Üyesi Meltem Kurt Pehlivanoğlu

Kocaeli Üniversitesi, Mühendislik Fakültesi,
Bilgisayar Mühendisliği Bölümü, Kocaeli

Meltem Kurt Pehlivanoğlu, 2010 yılında Trakya Üniversitesi Bilgisayar Mühendisliği Bölümü'nden lisans, 2012 yılında aynı üniversitenin Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Bölümü'nden yüksek lisans, 2018 yılında ise Kocaeli Üniversitesi, Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Bölümü'nden doktora derecelerini almıştır. 2019 yılında The University of Sheffield, Security of Advanced Systems araştırma grubunda TÜBİTAK 2219 - Yurt Dışı Doktora Sonrası Araştırma Burs Programı kapsamında 8 ay modern şifreleme yöntemleri, hafif sıklet şifreler için verimli yayılım tabakaları tasarımı ve yan kanal saldırıları konuları üzerine araştırmalar yapmıştır.

2020 yılında Kocaeli Üniversitesi, Bilgisayar Mühendisliği Bölümü, Bilgisayar Yazılımı Ana Bilim Dalı'nda Dr. Öğr. Üyesi unvanını almıştır. Dr. Öğr. Üyesi Meltem Kurt Pehlivanoğlu, siber güvenlik için uygulamalı kriptografi, simetrik anahtarlı şifreleme teknikleri, makine öğrenmesi ve derin öğrenme konuları üzerine çalışmalarını sürdürmektedir. Çok sayıda ulusal ve uluslararası makale ve bildirisi bulunmaktadır. Hâlen; Kocaeli Üniversitesi Bilgisayar Mühendisliği Bölümü'nde görevini yürütmekte olup, bilgi güvenliği ve kriptografi, ağ güvenliği, mikroişlemciler konularında lisans ve yüksek lisans dersleri vermektedir.

Dr. Elif Bilge Kavun

Passau Üniversitesi, Bilgisayar Bilimleri ve Matematik Fakültesi,
Güvenli Akıllı Sistemler Kürsüsü, Almanya

Elif Bilge Kavun, 2008 yılında İzmir Yüksek Teknoloji Enstitüsü Elektronik ve Haberleşme Mühendisliği Bölümü'nden lisans, 2010 yılında Orta Doğu Teknik Üniversitesi Uygulamalı Matematik Enstitüsü Kriptografi Bölümü'nden yüksek lisans, 2015 yılında ise Ruhr Üniversitesi Bochum (Almanya) Elektronik ve Bilgisayar Mühendisliği Fakültesi Gömülü Güvenlik Kürsüsü'nden doktora derecelerini almıştır. 2014-2018 yılları arasında Almanya Münih'teki Infineon Technologies AG'de kriptografi uygulamaları üzerine sayısal tasarım mühendisi olarak görev yapmıştır. 2019 yılında doktor öğretim üyesi olarak Sheffield Üniversitesi Bilgisayar Bilimleri Bölümü'ne geçmiş ve Gelişmiş Sistemlerin Güvenliği araştırma grubunda görev almıştır. 2020 yılı Ekim ayı itibarı ile akademik çalışmalarına Passau Üniversitesi'nde doktor öğretim üyesi olarak devam etmekte ve burada Güvenli Akıllı Sistemler Kürsüsü'nü yönetmektedir. Kriptografik uygulamaların gerçeklenmesi, bilgisayarlar ve gömülü sistemlerin güvenliği, donanım güvenliği ve akıllı sistemlerin güvenliği konularında dersler vermektedir. İlgilendiği araştırma konuları arasında (hafifsıklet) şifreleme teknikleri, donanım platformlarında şifreleme uygulamaları, donanım güvenliği, şifreleme sistemlerini hedef alan fiziksel saldırılar ile bunları önleme yöntemleri ve akıllı sistemlerin güvenliği yer almaktadır.

Ensar Şeker

Ensar Şeker lisans ve yüksek lisansını New York Institute of Technology Üniversitesinde elektronik ve bilgisayar mühendisliği alanında tamamlamış olup Tallinn University of Technology'de bilişim ve iletişim teknolojileri ana dalında doktorasına devam etmiştir. 2016 - 2018 yılları arasında merkezi Talin, Estonya'da bulunan NATO Müşterek Siber Savunma Mükemmeliyet Merkezi'nde ulusal temsilci olarak görev yapmıştır. 2015 - 2020 (Ekim) yılları arası TÜBİTAK BİLGEM bünyesinde uzman araştırmacı olarak çalışmıştır. Şu an özel bir şirkette siber güvenlik proje yöneticisi olarak çalışmalarına devam etmekte ve NATO, Avrupa Birliği gibi uluslararası organizasyonlarda da aktif görevlerini yürütmektedir. Siber güvenlik, yapay zekâ ve blokzincir konularında yayınlanmış birçok akademik makale ve yazısı bulunmakta olup, uluslararası birçok rapora katkı sağlamıştır.

Murat Kaya

Arkas Holding – Bimar A.Ş. Yazılım ve
Uygulama Güvenlik Uzmanı

20 yılı aşkın süredir çeşitli ulusal ve uluslararası sektörlerde Bilgi Sistemleri Yöneticiliği, Bilgi Güvenliği ve Bilişimde Kalite Danışmanlığı, Uygulama Geliştiricisi, Proje Yöneticisi, Eğitmen ve Analist olarak görev alan Murat Kaya, yaklaşık 12 yıldır Arkas Holding / Bimar A.Ş.'de Yazılım ve Bilgi Güvenliği Uzmanı olarak görev yapmaktadır.

Aktif olarak güvenli uygulama geliştirimi ve siber güvenlik odaklı çalışmalarına devam etmekte olup, DevSecOps ve Siber Güvenlik kültürünün benimsenmesi, yaygınlaştırılması ve geliştirilmesi konularında akademik ve sosyal organizasyonlarda gönüllü olarak yer almaktadır.

9-22 Nisan 2012 İnternet Haftası etkinliklerinde Ege bölgesinde ilk defa çocuklara özel ve yaş aralığına göre kategorilendirilmiş, veli ve yöneticilere ayrı olacak şekilde, "Çocuklar için Güvenli İnternet" eğitimleri/sunumları gerçekleştirmiş olup yaklaşık 3000 katılımcının bu eğitimlerden faydalanmasını sağlamıştır.

Doç. Dr. Tuğkan Tuğlular

İzmir Yüksek Teknoloji Enstitüsü
Bilgisayar Mühendisliği Bölümü

Tuğkan Tuğlular lisans, yüksek lisans ve doktora derecelerini Ege Üniversitesi Bilgisayar Mühendisliği'nden almıştır. Doktora çalışmaları sırasında ABD'nde Purdue Üniversitesi'nde araştırmacı olarak bulunmuştur. 2000 yılında İzmir Yüksek Teknoloji Enstitüsü'nde Yardımcı Doçent olmuştur. 2003-2007 yılları arasında aynı üniversitede Bilgiişlem Yöneticiliği yapan Tuğlular, 2010-2014 yılları arasında Bilgi Teknolojileri Rektör Danışmanı olarak görev yapmıştır. 2012 yılında İzmir'de gerçekleştirilen 40 ülkeden 450 kişinin katıldığı Bilgisayar Yazılım ve Uygulamaları Konferansı'nda (Computer Software Applications Conference - COMPSAC) Organizasyon Komitesi Başkanlığı görevini yürütmüştür. Aynı yıl İzmir Kalkınma Ajansı tarafından tanımlanan "İzmir Bilgi Toplumu Temelli Kalkınma Stratejisi" proje liderliği görevini üstlenmiştir. 2013-2018 yılları arasında İzmir tekno-girişimcilik ekosistemin güçlenmesi için yoğun olarak çalışmıştır. 2018 yılında Doçentlik unvanını alan Tuğkan Tuğlular, İzmir Yüksek Teknoloji Enstitüsü'nde hem Bilgisayar Mühendisliği Anabilim Dalı'nda hem de Teknoloji, Tasarım ve İnovasyon Yönetimi Anabilim Dalı'nda görev almaktadır. Akademik uzmanlık alanları arasında bilgi güvenliği, yazılım kalite güvence süreci, yazılım sınama ve güvenilir yazılım geliştirme olan Tuğkan Tuğlular'ın yetmiş beşin üzerinde ulusal ve uluslararası yayını bulunmaktadır.

İsmail Erkek

Bilgi Teknolojileri ve İletişim Kurumu,
Elektrik Elektronik Mühendisi, Ankara

2013 yılında Eskişehir Osmangazi Üniversitesi Elektrik Elektronik Mühendisliği'nden lisans derecesini tamamlayan İsmail ERKEK, 2018 yılında Gazi Üniversitesi Bilgi Güvenliği Mühendisliği Ana Bilim Dalı'nda yüksek lisans derecesini tamamlamıştır. 2020 yılında Gazi Üniversitesi Bilgi Güvenliği Mühendisliği Ana Bilim Dalı'nda doktora eğitimine devam etmektedir. İsmail ERKEK siber güvenlik sektöründe farklı kurumlarda siber güvenlik danışmanı olarak görev yapmış, 2019 yılından itibaren Bilgi Teknolojileri ve İletişim Kurumu bünyesinde siber güvenlik faaliyetleri yürütmektedir. Siber güvenlikte endüstriyel kontrol sistemleri güvenliği konularında uzmanlığı vardır.

Prof. Dr. Erdal Irmak

1975 Ankara doğumlu olan Prof. Dr. Erdal Irmak, lisans eğitimini Gazi Üniversitesi Teknik Eğitim Fakültesi Elektrik Eğitimi Bölümü'nde Temmuz 1997'de tamamladı. Ocak-2001'de Gazi Üniversitesi Fen Bilimleri Enstitüsü Elektrik Eğitimi Ana Bilim Dalı'nda, "Bilgisayar Kontrollü Bina Güvenlik Sisteminin Tasarımı ve Uygulaması" konulu yüksek lisans tezini tamamladı. Aynı Ana Bilim Dalında Temmuz 2007'de, "Uzaktan Eğitim Amaçlı İnternet Tabanlı Laboratuvar Uygulaması" konulu bir Doktora tezi hazırlayarak Doktor unvanı aldı.

Gazi Üniversitesi Teknik Eğitim Fakültesi Elektrik Eğitimi Bölümü'nde 1998-2007 yılları arasında Araştırma Görevlisi, 2007-2009 yılları arasında Öğretim Görevlisi, 2009-2011 yılları arasında Yrd. Doç. Dr. olarak görev yaptı. Gazi Üniversitesi Teknoloji Fakültesi Elektrik Elektronik Mühendisliği Bölümü'nde 2011-2013 yılları arasında Yrd. Doç. Dr. ve 2013-2019 yılları arasında Doç. Dr. olarak görev yapan Dr. Irmak, 2019 yılından itibaren aynı bölümde Prof. Dr. unvanıyla görevine devam etmektedir.

Elektrik güç sistemleri, akıllı şebekeler, yenilenebilir enerji sistemleri ve siber güvenlik konularında çalışmalar yapan Prof. Dr. Irmak'ın ulusal ve uluslararası dergilerde yayınlanmış 100'den fazla makale ve konferans bildirileri bulunmaktadır. Ayrıca iki adet uluslararası ve iki adet ulusal dergide editörlük görevi yürütmektedir.

Samime Meral

Uzman,

Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurumu
Bilgi Sistemleri Yönetimi Daire Başkanlığı

1991 İstanbul doğumludur. 2013 Süleyman Demirel Üniversitesi Bilgisayar Mühendisliği Bölümü mezunudur. Çalışma hayatına 2015 yılında Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurumunda uzman yardımcısı olarak başlamış, 2018 yılında uzmanlığını almıştır. 2019 yılında Gazi Üniversitesi Fen Bilimleri Enstitüsü Bilgi Güvenliği Mühendisliği Ana Bilim Dalında yüksek lisans eğitimine başlamış ve şu an tez aşamasındadır. Hâlen Kamu Gözetimi Muhasebe ve Denetim Standartları Kurumunda uzman olarak görev yapmaktadır.

Prof. Dr. Halil İbrahim Bülbül

Gazi Üniversitesi, Gazi Eğitim Fakültesi,
Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü Öğretim Üyesi

Araştırma ve çalışma alanları arasında Bilişim sistemleri, eğitim teknolojileri, e-öğrenme, web tabanlı eğitim, uzaktan eğitim, eğitim yazılımı tasarımı, makine öğrenmesi, veri madenciliği, bilgi güvenliği, siber güvenlik, yenilenebilir enerji sistemleri, ISO 9001 Kalite Yönetim Sistemi, meslek standartları ve mesleki yeterlikler vb. konular bulunmaktadır.

Yukarıda bahsedilen konularla ilgili kitap, makale vb. çeşitli yayınları ve ICMLA, ICRERA, SMART GRIDS vb. düzenlediği Ulusal ve Uluslararası düzeyde Konferanslarda düzenleme kurulu üyesi görevleri bulunmaktadır. Devlet ve özel sektör tarafından desteklenen ulusal ve uluslararası düzeyde çeşitli projeleri yürütmüştür. Tübitak, Sanayi Bakanlığı, KOSGEB, Ulusal ajans vb. kuruluşlarda hakem, panelist ve Komisyon Üyesi vb. görevleri yürütmektedir.

Hâlen Gazi Üniversitesi, Gazi Eğitim Fakültesinde Öğretim Üyesi olarak görev yapmakta, Yüksek Öğretim Başkanlığı (YÖK) Uzaktan Eğitim Komisyonu üyesi olarak ayrıca Hoca Ahmet Yesevi Üniversitesi, Uzaktan Eğitim Programları (TÜRTEP) Başkanı olarak görev yapmaktadır.

Dr. Öğr. Üyesi Yavuz Canbay

yavuzcanbay@ksu.edu.tr

Gazi Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Ana Bilim Dalı'nda doktorasını tamamladı.

Hâlen Kahramanmaraş Sütçü İmam Üniversitesi Bilgisayar Mühendisliği Bölümü'nde öğretim üyesi olarak görev yapmaktadır.

Veri Mahremiyeti, Siber Güvenlik, Büyük Veri, Veri Bilimi konularında çalışmakta olup Kahramanmaraş Sütçü İmam Üniversitesi Data Vision Laboratuvarının (datavision.ksu.edu.tr) yürütücülüğünü yapmaktadır.